

CIS Microsoft Windows Server 2016 STIG Benchmark

v3.0.0 - 08-26-2024

Terms of Use

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

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

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

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

Table of Contents

Terms of Use	1
Table of Contents	2
Overview	27
Important Usage Information	27
Target Technology Details	29
Intended Audience.....	29
Consensus Guidance	30
Typographical Conventions.....	31
Recommendation Definitions.....	32
Title	32
Assessment Status.....	32
Automated	32
Manual.....	32
Profile	32
Description.....	32
Rationale Statement	32
Impact Statement.....	33
Audit Procedure.....	33
Remediation Procedure.....	33
Default Value.....	33
References	33
CIS Critical Security Controls® (CIS Controls®)	33
Additional Information.....	33
Profile Definitions	34
Acknowledgements	37
Recommendations	38
1 Account Policies.....	38
1.1 Password Policy	38
1.1.1 Ensure 'Enforce password history' is set to '24 or more password(s)' (Automated)	39
1.1.2 Ensure 'Maximum password age' is set to '365 or fewer days, but not 0' (Automated) ..	42
1.1.3 Ensure 'Maximum password age' is set to '60 or fewer days, but not 0' (STIG only) (Automated)	44
1.1.4 Ensure 'Minimum password age' is set to '1 or more day(s)' (Automated).....	47
1.1.5 Ensure 'Minimum password length' is set to '14 or more character(s)' (Automated)	49
1.1.6 Ensure 'Password must meet complexity requirements' is set to 'Enabled' (Automated)	52
1.1.7 Ensure 'Store passwords using reversible encryption' is set to 'Disabled' (Automated) .	55

1.2 Account Lockout Policy	57
1.2.1 Ensure 'Account lockout duration' is set to '15 or more minute(s)' (Automated)	58
1.2.2 Ensure 'Account lockout threshold' is set to '5 or fewer invalid logon attempt(s), but not 0' (Automated)	61
1.2.3 Ensure 'Account lockout threshold' is set to '3 or fewer invalid logon attempt(s), but not 0' (STIG only) (Automated).....	63
1.2.4 Ensure 'Allow Administrator account lockout' is set to 'Enabled' (MS only) (Manual)	65
1.2.5 Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)' (Automated)	67
1.3 Kerberos Policy.....	70
1.3.1 Ensure 'Enforce user logon restrictions' is set to 'Enabled' (STIG DC only) (Manual)	71
1.3.2 Ensure 'Maximum lifetime for service ticket' is set to '600 or fewer minutes, but not 0' (STIG DC only) (Manual)	72
1.3.3 Ensure 'Maximum lifetime for user ticket' is set to '10 or fewer hours, but not 0' (STIG DC only) (Manual)	74
1.3.4 Ensure 'Maximum lifetime for user ticket renewal' is set to '7 or fewer days' (STIG DC only) (Manual)	76
1.3.5 Ensure 'Maximum tolerance for computer clock synchronization' is set to '5 or fewer minutes' (STIG DC only) (Manual).....	77
2 Local Policies.....	79
2.1 Audit Policy	79
2.2 User Rights Assignment	79
2.2.1 Ensure 'Access Credential Manager as a trusted caller' is set to 'No One' (Automated) 80	
2.2.2 Ensure 'Access this computer from the network' is set to 'Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS' (DC only) (Automated)	82
2.2.3 Ensure 'Access this computer from the network' is set to 'Administrators, Authenticated Users' (MS only) (Automated).....	84
2.2.4 Ensure 'Act as part of the operating system' is set to 'No One' (Automated)	86
2.2.5 Ensure 'Add workstations to domain' is set to 'Administrators' (DC only) (Automated) ..	88
2.2.6 Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE' (Automated)	90
2.2.7 Ensure 'Allow log on locally' is set to 'Administrators, ENTERPRISE DOMAIN CONTROLLERS' (DC only) (Automated)	92
2.2.8 Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators' (DC only) (Automated)	94
2.2.9 Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators, Remote Desktop Users' (MS only) (Automated).....	96
2.2.10 Ensure 'Back up files and directories' is set to 'Administrators' (Automated)	98
2.2.11 Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE' (Automated)	100
2.2.12 Ensure 'Change the time zone' is set to 'Administrators, LOCAL SERVICE' (Automated)	103
2.2.13 Ensure 'Create a pagefile' is set to 'Administrators' (Automated)	105
2.2.14 Ensure 'Create a token object' is set to 'No One' (Automated)	107
2.2.15 Ensure 'Create global objects' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (Automated).....	109
2.2.16 Ensure 'Create permanent shared objects' is set to 'No One' (Automated)	111
2.2.17 Ensure 'Create symbolic links' is set to 'Administrators' (DC only) (Automated).....	113
2.2.18 Ensure 'Create symbolic links' is set to 'Administrators, NT VIRTUAL MACHINE\Virtual Machines' (MS only) (Automated).....	115
2.2.19 Ensure 'Debug programs' is set to 'Administrators' (Automated)	117
2.2.20 Ensure 'Deny access to this computer from the network' to include 'Guests' (DC only) (Automated)	119
2.2.21 Ensure 'Deny access to this computer from the network' to include 'Guests, Local account and member of Administrators group' (MS only) (Automated).....	121

2.2.22 Ensure 'Deny access to this computer from the network' to include 'Guests, Enterprise Admins Group, Domains Admins Group, Local account, and member of Administrators group' (STIG MS only) (Automated)	123
2.2.23 Ensure 'Deny log on as a batch job' to include 'Guests' (Automated)	125
2.2.24 Ensure 'Deny log on as a batch job' to include 'Guests, Enterprise Admins Group, and Domain Admins Group' (STIG MS only) (Automated)	127
2.2.25 Ensure 'Deny log on as a service' to include 'Guests' (Automated)	129
2.2.26 Ensure 'Deny log on as a service' to include 'No one' (STIG DC only) (Automated) ..	131
2.2.27 Ensure 'Deny log on as a service' to include 'Enterprise Admins Group and Domain Admins Group' (STIG MS only) (Automated)	133
2.2.28 Ensure 'Deny log on locally' to include 'Guests' (Automated)	135
2.2.29 Ensure 'Deny log on locally' to include 'Guests, Enterprise Admins group, and Domain Admins group' (STIG MS only) (Automated)	137
2.2.30 Ensure 'Deny log on through Remote Desktop Services' to include 'Guests' (DC only) (Automated)	139
2.2.31 Ensure 'Deny log on through Remote Desktop Services' is set to 'Guests, Local account' (MS only) (Automated)	141
2.2.32 Ensure 'Deny log on through Remote Desktop Services' is set to 'Guests, Local account, Enterprise Admins Group, and Domain Admins Group' (STIG MS only) (Automated)	143
2.2.33 Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'Administrators' (DC only) (Automated)	145
2.2.34 Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'No One' (MS only) (Automated)	147
2.2.35 Ensure 'Force shutdown from a remote system' is set to 'Administrators' (Automated)	149
2.2.36 Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE' (Automated)	151
2.2.37 Ensure 'Impersonate a client after authentication' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (DC only) (Automated)	153
2.2.38 Ensure 'Impersonate a client after authentication' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' and (when the Web Server (IIS) Role with Web Services Role Service is installed) 'IIS_IUSRS' (MS only) (Automated)	155
2.2.39 Ensure 'Impersonate a client after authentication' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (STIG MS only) (Automated)	157
2.2.40 Ensure 'Increase scheduling priority' is set to 'Administrators' (Automated)	159
2.2.41 Ensure 'Load and unload device drivers' is set to 'Administrators' (Automated)	161
2.2.42 Ensure 'Lock pages in memory' is set to 'No One' (Automated)	163
2.2.43 Ensure 'Log on as a batch job' is set to 'Administrators' (DC Only) (Automated)	165
2.2.44 Ensure 'Manage auditing and security log' is set to 'Administrators' (DC only) (Automated)	167
2.2.45 Ensure 'Manage auditing and security log' is set to 'Administrators' (MS only) (Automated)	169
2.2.46 Ensure 'Manage auditing and security log' is set to 'Administrators' (STIG DC only) (Automated)	171
2.2.47 Ensure 'Modify an object label' is set to 'No One' (Automated)	173
2.2.48 Ensure 'Modify firmware environment values' is set to 'Administrators' (Automated) ..	175
2.2.49 Ensure 'Perform volume maintenance tasks' is set to 'Administrators' (Automated) ..	177
2.2.50 Ensure 'Profile single process' is set to 'Administrators' (Automated)	179
2.2.51 Ensure 'Profile system performance' is set to 'Administrators, NT SERVICE\WdiServiceHost' (Automated)	181
2.2.52 Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE' (Automated)	183
2.2.53 Ensure 'Restore files and directories' is set to 'Administrators' (Automated)	185
2.2.54 Ensure 'Shut down the system' is set to 'Administrators' (Automated)	187

2.2.55 Ensure 'Synchronize directory service data' is set to 'No One' (DC only) (Automated)	189
2.2.56 Ensure 'Take ownership of files or other objects' is set to 'Administrators' (Automated)	191
2.3 Security Options	193
2.3.1 Accounts	193
2.3.1.1 Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts' (Automated)	194
2.3.1.2 Ensure 'Accounts: Guest account status' is set to 'Disabled' (MS only) (Automated)	196
2.3.1.3 Ensure 'Accounts: Guest account status' is set to 'Disabled' (STIG only) (Automated)	198
2.3.1.4 Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled' (Automated)	200
2.3.1.5 Configure 'Accounts: Rename administrator account' (Automated)	202
2.3.1.6 Configure 'Accounts: Rename guest account' (Automated)	204
2.3.2 Audit	206
2.3.2.1 Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled' (Automated)	207
2.3.2.2 Ensure 'Audit: Shut down system immediately if unable to log security audits' is set to 'Disabled' (Automated)	210
2.3.3 DCOM	212
2.3.4 Devices	212
2.3.4.1 Ensure 'Devices: Prevent users from installing printer drivers' is set to 'Enabled' (Automated)	213
2.3.5 Domain controller	215
2.3.5.1 Ensure 'Domain controller: Allow server operators to schedule tasks' is set to 'Disabled' (DC only) (Automated)	216
2.3.5.2 Ensure 'Domain controller: Allow vulnerable Netlogon secure channel connections' is set to 'Not Configured' (DC Only) (Automated)	218
2.3.5.3 Ensure 'Domain controller: LDAP server channel binding token requirements' is set to 'Always' (DC Only) (Automated)	220
2.3.5.4 Ensure 'Domain controller: LDAP server signing requirements' is set to 'Require signing' (DC only) (Automated)	223
2.3.5.5 Ensure 'Domain controller: Refuse machine account password changes' is set to 'Disabled' (DC only) (Automated)	226
2.3.6 Domain member	228
2.3.6.1 Ensure 'Domain member: Digitally encrypt or sign secure channel data (always)' is set to 'Enabled' (Automated)	229
2.3.6.2 Ensure 'Domain member: Digitally encrypt secure channel data (when possible)' is set to 'Enabled' (Automated)	232
2.3.6.3 Ensure 'Domain member: Digitally sign secure channel data (when possible)' is set to 'Enabled' (Automated)	234
2.3.6.4 Ensure 'Domain member: Disable machine account password changes' is set to 'Disabled' (Automated)	236
2.3.6.5 Ensure 'Domain member: Maximum machine account password age' is set to '30 or fewer days, but not 0' (Automated)	238
2.3.6.6 Ensure 'Domain member: Require strong (Windows 2000 or later) session key' is set to 'Enabled' (Automated)	240
2.3.7 Interactive logon	242
2.3.7.1 Ensure 'Interactive logon: Do not display last user name' is set to 'Enabled' (Automated)	243
2.3.7.2 Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled' (Automated)	245
2.3.7.3 Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0' (Automated)	247

2.3.7.4 Configure 'Interactive logon: Message text for users attempting to log on' (Automated)	249
2.3.7.5 Configure 'Interactive logon: Message title for users attempting to log on' (Automated)	252
2.3.7.6 Ensure 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' is set to '4 or fewer logon(s)' (MS only) (Automated)	254
2.3.7.7 Ensure 'Interactive logon: Prompt user to change password before expiration' is set to 'between 5 and 14 days' (Automated)	256
2.3.7.8 Ensure 'Interactive logon: Require Domain Controller Authentication to unlock workstation' is set to 'Enabled' (MS only) (Automated)	258
2.3.7.9 Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher (Automated)	260
2.3.7.10 Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or 'Force Logoff' (STIG only) (Automated)	262
2.3.8 Microsoft network client	265
2.3.8.1 Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled' (Automated)	266
2.3.8.2 Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled' (Automated)	269
2.3.8.3 Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled' (Automated)	272
2.3.9 Microsoft network server	274
2.3.9.1 Ensure 'Microsoft network server: Amount of idle time required before suspending session' is set to '15 or fewer minute(s)' (Automated)	275
2.3.9.2 Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled' (Automated)	277
2.3.9.3 Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled' (Automated)	280
2.3.9.4 Ensure 'Microsoft network server: Disconnect clients when logon hours expire' is set to 'Enabled' (Automated)	283
2.3.9.5 Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher (MS only) (Automated)	285
2.3.10 Network access	288
2.3.10.1 Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled' (Automated)	289
2.3.10.2 Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled' (MS only) (Automated)	291
2.3.10.3 Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled' (STIG only) (Automated)	293
2.3.10.4 Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled' (MS only) (Automated)	295
2.3.10.5 Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled' (STIG only) (Automated)	297
2.3.10.6 Ensure 'Network access: Do not allow storage of passwords and credentials for network authentication' is set to 'Enabled' (Automated)	299
2.3.10.7 Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled' (Automated)	301
2.3.10.8 Configure 'Network access: Named Pipes that can be accessed anonymously' (DC only) (Automated)	303
2.3.10.9 Configure 'Network access: Named Pipes that can be accessed anonymously' (MS only) (Automated)	305
2.3.10.10 Configure 'Network access: Remotely accessible registry paths' is configured (Automated)	307
2.3.10.11 Configure 'Network access: Remotely accessible registry paths and sub-paths' is configured (Automated)	309

2.3.10.12 Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled' (Automated)	313
2.3.10.13 Ensure 'Network access: Restrict clients allowed to make remote calls to SAM' is set to 'Administrators: Remote Access: Allow' (MS only) (Automated)	316
2.3.10.14 Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None' (Automated)	318
2.3.10.15 Ensure 'Network access: Sharing and security model for local accounts' is set to 'Classic - local users authenticate as themselves' (Automated)	320
2.3.11 Network security	322
2.3.11.1 Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled' (Automated)	323
2.3.11.2 Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled' (Automated)	325
2.3.11.3 Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled' (Automated)	327
2.3.11.4 Ensure 'Network security: Configure encryption types allowed for Kerberos' is set to 'AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types' (Automated)	329
2.3.11.5 Ensure 'Network security: Do not store LAN Manager hash value on next password change' is set to 'Enabled' (Automated)	332
2.3.11.6 Ensure 'Network security: Force logoff when logon hours expire' is set to 'Enabled' (Manual)	334
2.3.11.7 Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM' (Automated)	336
2.3.11.8 Ensure 'Network security: LDAP client signing requirements' is set to 'Negotiate signing' or higher (Automated)	339
2.3.11.9 Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit encryption' (Automated)	341
2.3.11.10 Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption' (Automated)	343
2.3.11.11 Ensure 'Network security: Restrict NTLM: Audit Incoming NTLM Traffic' is set to 'Enable auditing for all accounts' (Automated)	345
2.3.11.12 Ensure 'Network security: Restrict NTLM: Audit NTLM authentication in this domain' is set to 'Enable all' (DC only) (Automated)	347
2.3.11.13 Ensure 'Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers' is set to 'Audit all' or higher (Automated)	349
2.3.12 Recovery console	351
2.3.13 Shutdown	351
2.3.13.1 Ensure 'Shutdown: Allow system to be shut down without having to log on' is set to 'Disabled' (Automated)	352
2.3.14 System cryptography	354
2.3.14.1 Ensure 'System cryptography: Force strong key protection for user keys stored on the computer' is set to 'User must enter a password each time they use a key' (STIG only) (Automated)	355
2.3.14.2 Ensure 'System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing' is set to 'Enabled' (STIG only) (Automated)	357
2.3.15 System objects	360
2.3.15.1 Ensure 'System objects: Require case insensitivity for non-Windows subsystems' is set to 'Enabled' (Automated)	361
2.3.15.2 Ensure 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)' is set to 'Enabled' (Automated)	363
2.3.16 System settings	365
2.3.17 User Account Control	365
2.3.17.1 Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled' (Automated)	366

2.3.17.2 Ensure 'User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop' is set to 'Disabled' (STIG only) (Automated)	368
2.3.17.3 Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop' or higher (Automated)	370
2.3.17.4 Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests' (Automated)	372
2.3.17.5 Ensure 'User Account Control: Detect application installations and prompt for elevation' is set to 'Enabled' (Automated)	374
2.3.17.6 Ensure 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' is set to 'Enabled' (Automated)	376
2.3.17.7 Ensure 'User Account Control: Run all administrators in Admin Approval Mode' is set to 'Enabled' (Automated)	378
2.3.17.8 Ensure 'User Account Control: Switch to the secure desktop when prompting for elevation' is set to 'Enabled' (Automated)	380
2.3.17.9 Ensure 'User Account Control: Virtualize file and registry write failures to per-user locations' is set to 'Enabled' (Automated)	382
3 Event Log	384
4 Restricted Groups	384
5 System Services	384
5.1 Ensure 'Microsoft FTP Service (FTPSVC)' is set to 'Not Installed' (STIG only) (Automated)	385
5.2 Ensure 'Peer Name Resolution Protocol (PNRPsvc)' is set to 'Not Installed' (STIG only) (Automated)	387
5.3 Ensure 'Print Spooler (Spooler)' is set to 'Disabled' (DC only) (Automated)	389
5.4 Ensure 'Print Spooler (Spooler)' is set to 'Disabled' (MS only) (Automated)	391
5.5 Ensure 'Simple TCP/IP Services (simptcp)' is set to 'Not Installed' (Automated)	393
6 Registry	395
7 File System	395
8 Wired Network (IEEE 802.3) Policies	395
9 Windows Defender Firewall with Advanced Security (formerly Windows Firewall with Advanced Security)	395
9.1 Domain Profile	395
9.1.1 Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)' (Automated)	396
9.1.2 Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)' (Automated)	398
9.1.3 Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)' (STIG only) (Automated)	400
9.1.4 Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No' (Automated)	402
9.1.5 Ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\domainfw.log' (Automated)	404
9.1.6 Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater' (Automated)	406
9.1.7 Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes' (Automated)	408
9.1.8 Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes' (Automated)	410
9.2 Private Profile	412

9.2.1 Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)' (Automated)	413
9.2.2 Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)' (Automated)	415
9.2.3 Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)' (STIG only) (Automated)	417
9.2.4 Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No' (Automated)	419
9.2.5 Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\privatefw.log' (Automated)	421
9.2.6 Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater' (Automated)	423
9.2.7 Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes' (Automated)	425
9.2.8 Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes' (Automated)	427
9.3 Public Profile	429
9.3.1 Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)' (Automated)	430
9.3.2 Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)' (Automated)	432
9.3.3 Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)' (STIG only) (Automated)	434
9.3.4 Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'No' (Automated)	436
9.3.5 Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No' (Automated)	438
9.3.6 Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No' (Automated)	440
9.3.7 Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\publicfw.log' (Automated)	442
9.3.8 Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater' (Automated)	444
9.3.9 Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes' (Automated)	446
9.3.10 Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes' (Automated)	448
10 Network List Manager Policies	450
11 Wireless Network (IEEE 802.11) Policies	450
12 Public Key Policies	450
13 Software Restriction Policies	450
14 Network Access Protection NAP Client Configuration	450
15 Application Control Policies	450
16 IP Security Policies	450
17 Advanced Audit Policy Configuration	451
17.1 Account Logon	451
17.1.1 Ensure 'Audit Credential Validation' is set to 'Success and Failure' (Automated)	452
17.1.2 Ensure 'Audit Kerberos Authentication Service' is set to 'Success and Failure' (DC Only) (Automated)	454
17.1.3 Ensure 'Audit Kerberos Service Ticket Operations' is set to 'Success and Failure' (DC Only) (Automated)	456

17.2 Account Management	458
17.2.1 Ensure 'Audit Application Group Management' is set to 'Success and Failure' (Automated)	459
17.2.2 Ensure 'Audit Computer Account Management' is set to include 'Success' (DC only) (Automated)	461
17.2.3 Ensure 'Audit Distribution Group Management' is set to include 'Success' (DC only) (Automated)	463
17.2.4 Ensure 'Audit Other Account Management Events' is set to include 'Success' (DC only) (Automated)	465
17.2.5 Ensure 'Audit Other Account Management Events' is set to include 'Success' (STIG Only) (Automated)	467
17.2.6 Ensure 'Audit Security Group Management' is set to include 'Success' (Automated)	469
17.2.7 Ensure 'Audit User Account Management' is set to 'Success and Failure' (Automated)	472
17.3 Detailed Tracking	475
17.3.1 Ensure 'Audit PNP Activity' is set to include 'Success' (Automated)	476
17.3.2 Ensure 'Audit Process Creation' is set to include 'Success' (Automated)	478
17.4 DS Access	480
17.4.1 Ensure 'Audit Directory Service Access' is set to include 'Failure' (DC only) (Automated)	481
17.4.2 Ensure 'Audit Directory Service Access' is set to include 'Success and Failure' (STIG DC only) (Automated)	483
17.4.3 Ensure 'Audit Directory Service Changes' is set to include 'Success' (DC only) (Automated)	485
17.5 Logon/Logoff	487
17.5.1 Ensure 'Audit Account Lockout' is set to include 'Failure' (Automated)	488
17.5.2 Ensure 'Audit Group Membership' is set to include 'Success' (Automated)	490
17.5.3 Ensure 'Audit Logoff' is set to include 'Success' (Automated)	492
17.5.4 Ensure 'Audit Logon' is set to 'Success and Failure' (Automated)	494
17.5.5 Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure' (Automated)	496
17.5.6 Ensure 'Audit Special Logon' is set to include 'Success' (Automated)	498
17.6 Object Access	500
17.6.1 Ensure 'Audit Detailed File Share' is set to include 'Failure' (Automated)	501
17.6.2 Ensure 'Audit File Share' is set to 'Success and Failure' (Automated)	503
17.6.3 Ensure 'Audit Other Object Access Events' is set to 'Success and Failure' (Automated)	505
17.6.4 Ensure 'Audit Removable Storage' is set to 'Success and Failure' (Automated)	507
17.7 Policy Change	509
17.7.1 Ensure 'Audit Audit Policy Change' is set to include 'Success' (Automated)	510
17.7.2 Ensure 'Audit Audit Policy Change' is set to include 'Success and Failure' (STIG only) (Automated)	512
17.7.3 Ensure 'Audit Authentication Policy Change' is set to include 'Success' (Automated)	514
17.7.4 Ensure 'Audit Authorization Policy Change' is set to include 'Success' (Automated)	517
17.7.5 Ensure 'Audit MPSSVC Rule-Level Policy Change' is set to 'Success and Failure' (Automated)	520
17.7.6 Ensure 'Audit Other Policy Change Events' is set to include 'Failure' (Automated)	522
17.8 Privilege Use	524
17.8.1 Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure' (Automated)	525
17.9 System	528
17.9.1 Ensure 'Audit IPsec Driver' is set to 'Success and Failure' (Automated)	529
17.9.2 Ensure 'Audit Other System Events' is set to 'Success and Failure' (Automated)	532
17.9.3 Ensure 'Audit Security State Change' is set to include 'Success' (Automated)	535
17.9.4 Ensure 'Audit Security System Extension' is set to include 'Success' (Automated)	537
17.9.5 Ensure 'Audit System Integrity' is set to 'Success and Failure' (Automated)	539

18 Administrative Templates (Computer)	541
18.1 Control Panel	541
18.1.1 Personalization	541
18.1.1.1 Ensure 'Prevent enabling lock screen camera' is set to 'Enabled' (Automated)	542
18.1.1.2 Ensure 'Prevent enabling lock screen slide show' is set to 'Enabled' (Automated)	544
18.1.2 Regional and Language Options	546
18.1.2.1 Handwriting personalization	546
18.1.2.2 Ensure 'Allow users to enable online speech recognition services' is set to 'Disabled' (Automated)	547
18.1.3 Ensure 'Allow Online Tips' is set to 'Disabled' (Automated)	549
18.2 Desktop	551
18.3 LAPS (legacy)	551
18.3.1 Ensure LAPS AdmPwd GPO Extension / CSE is installed (MS only) (Automated)	552
18.3.2 Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled' (MS only) (Automated)	555
18.3.3 Ensure 'Enable Local Admin Password Management' is set to 'Enabled' (MS only) (Automated)	557
18.3.4 Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + special characters' (MS only) (Automated)	560
18.3.5 Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more' (MS only) (Automated)	562
18.3.6 Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer' (MS only) (Automated)	564
18.3.7 Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 60 or fewer' (STIG MS only) (Automated)	566
18.4 MS Security Guide	568
18.4.1 Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled' (MS only) (Automated)	569
18.4.2 Ensure 'Configure RPC packet level privacy setting for incoming connections' is set to 'Enabled' (Automated)	571
18.4.3 Ensure 'Configure SMB v1 client driver' is set to 'Enabled: Disable driver (recommended)' (Automated)	573
18.4.4 Ensure 'Configure SMB v1 server' is set to 'Disabled' (Automated)	576
18.4.5 Ensure 'Enable Certificate Padding' is set to 'Enabled' (Automated)	579
18.4.6 Ensure 'Enable Structured Exception Handling Overwrite Protection (SEHOP)' is set to 'Enabled' (Automated)	581
18.4.7 Ensure 'LSA Protection' is set to 'Enabled' (Automated)	583
18.4.8 Ensure 'NetBT NodeType configuration' is set to 'Enabled: P-node (recommended)' (Automated)	585
18.4.9 Ensure 'WDigest Authentication' is set to 'Disabled' (Automated)	587
18.5 MSS (Legacy)	589
18.5.1 Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon' is set to 'Disabled' (Automated)	590
18.5.2 Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level' is set to 'Enabled: Highest protection, source routing is completely disabled' (Automated)	592
18.5.3 Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level' is set to 'Enabled: Highest protection, source routing is completely disabled' (Automated)	594
18.5.4 Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled' (Automated)	596
18.5.5 Ensure 'MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds' is set to 'Enabled: 300,000 or 5 minutes' (Automated)	598
18.5.6 Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled' (Automated)	600
18.5.7 Ensure 'MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses' is set to 'Disabled' (Automated)	602

18.5.8 Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode' is set to 'Enabled' (Automated)	604
18.5.9 Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires' is set to 'Enabled: 5 or fewer seconds' (Automated)	606
18.5.10 Ensure 'MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3' (Automated)	608
18.5.11 Ensure 'MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3' (Automated).....	610
18.5.12 Ensure 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' is set to 'Enabled: 90% or less' (Automated)	612
18.6 Network	614
18.6.1 Background Intelligent Transfer Service (BITS)	614
18.6.2 BranchCache	614
18.6.3 DirectAccess Client Experience Settings	614
18.6.4 DNS Client.....	614
18.6.4.1 Ensure 'Configure NetBIOS settings' is set to 'Enabled: Disable NetBIOS name resolution on public networks' (Automated)	615
18.6.4.2 Ensure 'Turn off multicast name resolution' is set to 'Enabled' (Automated)	617
18.6.5 Fonts.....	619
18.6.5.1 Ensure 'Enable Font Providers' is set to 'Disabled' (Automated)	620
18.6.6 Hotspot Authentication	622
18.6.7 Lanman Server	622
18.6.8 Lanman Workstation.....	622
18.6.8.1 Ensure 'Enable insecure guest logons' is set to 'Disabled' (Automated).....	623
18.6.9 Link-Layer Topology Discovery.....	625
18.6.9.1 Ensure 'Turn on Mapper I/O (LLTDIO) driver' is set to 'Disabled' (Automated).....	626
18.6.9.2 Ensure 'Turn on Responder (RSPNDR) driver' is set to 'Disabled' (Automated)	628
18.6.10 Microsoft Peer-to-Peer Networking Services	630
18.6.10.1 Peer Name Resolution Protocol.....	630
18.6.10.2 Ensure 'Turn off Microsoft Peer-to-Peer Networking Services' is set to 'Enabled' (Automated)	631
18.6.11 Network Connections	633
18.6.11.1 Windows Defender Firewall (formerly Windows Firewall)	633
18.6.11.2 Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled' (Automated).....	634
18.6.11.3 Ensure 'Prohibit use of Internet Connection Sharing on your DNS domain network' is set to 'Enabled' (Automated).....	636
18.6.11.4 Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled' (Automated).....	638
18.6.12 Network Connectivity Status Indicator	640
18.6.13 Network Isolation	640
18.6.14 Network Provider.....	640
18.6.14.1 Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication", "Require Integrity", and "Require Privacy" set for all NETLOGON and SYSVOL shares' (Automated)	641
18.6.14.2 Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication", "Require Integrity" set for all NETLOGON and SYSVOL shares' (STIG only) (Automated)	643
18.6.15 Offline Files.....	645
18.6.16 QoS Packet Scheduler	645
18.6.17 SNMP	645
18.6.18 SSL Configuration Settings	645
18.6.19 TCPIP Settings.....	646
18.6.19.1 IPv6 Transition Technologies.....	646
18.6.19.2 Parameters	646

18.6.19.2.1 Disable IPv6 (Ensure TCPIP6 Parameter 'DisabledComponents' is set to '0xff (255)') (Automated)	647
18.6.20 Windows Connect Now	649
18.6.20.1 Ensure 'Configuration of wireless settings using Windows Connect Now' is set to 'Disabled' (Automated)	650
18.6.20.2 Ensure 'Prohibit access of the Windows Connect Now wizards' is set to 'Enabled' (Automated)	652
18.6.21 Windows Connection Manager	654
18.6.21.1 Ensure 'Minimize the number of simultaneous connections to the Internet or a Windows Domain' is set to 'Enabled: 1 = Minimize simultaneous connections' (Automated)	655
18.6.21.2 Ensure 'Prohibit connection to non-domain networks when connected to domain authenticated network' is set to 'Enabled' (MS only) (Automated)	657
18.7 Printers	659
18.7.1 Ensure 'Allow Print Spooler to accept client connections' is set to 'Disabled' (Automated)	660
18.7.2 Ensure 'Configure Redirection Guard' is set to 'Enabled: Redirection Guard Enabled' (Automated)	662
18.7.3 Ensure 'Configure RPC connection settings: Protocol to use for outgoing RPC connections' is set to 'Enabled: RPC over TCP' (Automated)	664
18.7.4 Ensure 'Configure RPC connection settings: Use authentication for outgoing RPC connections' is set to 'Enabled: Default' (Automated)	666
18.7.5 Ensure 'Configure RPC listener settings: Protocols to allow for incoming RPC connections' is set to 'Enabled: RPC over TCP' (Automated)	668
18.7.6 Ensure 'Configure RPC listener settings: Authentication protocol to use for incoming RPC connections' is set to 'Enabled: Negotiate' or higher (Automated)	670
18.7.7 Ensure 'Configure RPC over TCP port' is set to 'Enabled: 0' (Automated)	672
18.7.8 Ensure 'Limits print driver installation to Administrators' is set to 'Enabled' (Automated)	674
18.7.9 Ensure 'Manage processing of Queue-specific files' is set to 'Enabled: Limit Queue-specific files to Color profiles' (Automated)	676
18.7.10 Ensure 'Point and Print Restrictions: When installing drivers for a new connection' is set to 'Enabled: Show warning and elevation prompt' (Automated)	678
18.7.11 Ensure 'Point and Print Restrictions: When updating drivers for an existing connection' is set to 'Enabled: Show warning and elevation prompt' (Automated)	680
18.8 Start Menu and Taskbar	682
18.8.1 Notifications	682
18.8.1.1 Ensure 'Turn off notifications network usage' is set to 'Enabled' (Automated)	683
18.9 System	685
18.9.1 Access-Denied Assistance	685
18.9.2 App-V	685
18.9.3 Audit Process Creation	685
18.9.3.1 Ensure 'Include command line in process creation events' is set to 'Enabled' (Automated)	686
18.9.4 Credentials Delegation	689
18.9.4.1 Ensure 'Encryption Oracle Remediation' is set to 'Enabled: Force Updated Clients' (Automated)	690
18.9.4.2 Ensure 'Remote host allows delegation of non-exportable credentials' is set to 'Enabled' (Automated)	692
18.9.5 Device Guard	694
18.9.5.1 Ensure 'Turn On Virtualization Based Security' is set to 'Enabled' (Automated)	695
18.9.5.2 Ensure 'Turn On Virtualization Based Security: Select Platform Security Level' is set to 'Secure Boot' or higher (Automated)	698
18.9.5.3 Ensure 'Turn On Virtualization Based Security: Virtualization Based Protection of Code Integrity' is set to 'Enabled with UEFI lock' (Automated)	701
18.9.5.4 Ensure 'Turn On Virtualization Based Security: Require UEFI Memory Attributes Table' is set to 'True (checked)' (Automated)	703

18.9.5.5 Ensure 'Turn On Virtualization Based Security: Credential Guard Configuration' is set to 'Enabled with UEFI lock' (MS Only) (Automated)	705
18.9.5.6 Ensure 'Turn On Virtualization Based Security: Credential Guard Configuration' is set to 'Disabled' (DC Only) (Automated)	708
18.9.5.7 Ensure 'Turn On Virtualization Based Security: Secure Launch Configuration' is set to 'Enabled' (Automated)	710
18.9.6 Device Health Attestation Service	712
18.9.7 Device Installation	712
18.9.7.1 Device Installation Restrictions	712
18.9.7.2 Ensure 'Prevent device metadata retrieval from the Internet' is set to 'Enabled' (Automated)	713
18.9.8 Disk NV Cache	715
18.9.9 Disk Quotas	715
18.9.10 Display	715
18.9.11 Distributed COM	715
18.9.12 Driver Installation	715
18.9.13 Early Launch Antimalware	716
18.9.13.1 Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good, unknown and bad but critical' (Automated)	717
18.9.13.2 Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: any, but ALL' (STIG only) (Automated)	719
18.9.14 Enhanced Storage Access	721
18.9.15 File Classification Infrastructure	721
18.9.16 File Share Shadow Copy Provider	721
18.9.17 Filesystem (formerly NTFS Filesystem)	721
18.9.18 Folder Redirection	721
18.9.19 Group Policy	722
18.9.19.1 Logging and tracing	722
18.9.19.2 Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE' (Automated)	723
18.9.19.3 Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE' (Automated)	725
18.9.19.4 Ensure 'Configure security policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE' (Automated)	727
18.9.19.5 Ensure 'Configure security policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE' (Automated)	729
18.9.19.6 Ensure 'Continue experiences on this device' is set to 'Disabled' (Automated)	731
18.9.19.7 Ensure 'Turn off background refresh of Group Policy' is set to 'Disabled' (Automated)	733
18.9.20 Internet Communication Management	735
18.9.20.1 Internet Communication settings	735
18.9.20.1.1 Ensure 'Turn off downloading of print drivers over HTTP' is set to 'Enabled' (Automated)	736
18.9.20.1.2 Ensure 'Turn off handwriting personalization data sharing' is set to 'Enabled' (Automated)	738
18.9.20.1.3 Ensure 'Turn off handwriting recognition error reporting' is set to 'Enabled' (Automated)	740
18.9.20.1.4 Ensure 'Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com' is set to 'Enabled' (Automated)	742
18.9.20.1.5 Ensure 'Turn off Internet download for Web publishing and online ordering wizards' is set to 'Enabled' (Automated)	744
18.9.20.1.6 Ensure 'Turn off printing over HTTP' is set to 'Enabled' (Automated)	746
18.9.20.1.7 Ensure 'Turn off Registration if URL connection is referring to Microsoft.com' is set to 'Enabled' (Automated)	748
18.9.20.1.8 Ensure 'Turn off Search Companion content file updates' is set to 'Enabled' (Automated)	750

18.9.20.1.9 Ensure 'Turn off the "Order Prints" picture task' is set to 'Enabled' (Automated)	752
18.9.20.1.10 Ensure 'Turn off the "Publish to Web" task for files and folders' is set to 'Enabled' (Automated)	754
18.9.20.1.11 Ensure 'Turn off the Windows Messenger Customer Experience Improvement Program' is set to 'Enabled' (Automated)	756
18.9.20.1.12 Ensure 'Turn off Windows Customer Experience Improvement Program' is set to 'Enabled' (Automated)	758
18.9.20.1.13 Ensure 'Turn off Windows Error Reporting' is set to 'Enabled' (Automated)	760
18.9.21 iSCSI	762
18.9.22 KDC	762
18.9.23 Kerberos	762
18.9.23.1 Ensure 'Support device authentication using certificate' is set to 'Enabled: Automatic' (Automated)	763
18.9.24 Kernel DMA Protection	765
18.9.25 LAPS	765
18.9.26 Local Security Authority	765
18.9.27 Locale Services	765
18.9.27.1 Ensure 'Disallow copying of user input methods to the system account for sign-in' is set to 'Enabled' (Automated)	766
18.9.28 Logon	768
18.9.28.1 Ensure 'Block user from showing account details on sign-in' is set to 'Enabled' (Automated)	769
18.9.28.2 Ensure 'Do not display network selection UI' is set to 'Enabled' (Automated)	771
18.9.28.3 Ensure 'Do not enumerate connected users on domain-joined computers' is set to 'Enabled' (Automated)	773
18.9.28.4 Ensure 'Enumerate local users on domain-joined computers' is set to 'Disabled' (MS only) (Automated)	775
18.9.28.5 Ensure 'Turn off app notifications on the lock screen' is set to 'Enabled' (Automated)	777
18.9.28.6 Ensure 'Turn off picture password sign-in' is set to 'Enabled' (Automated)	779
18.9.28.7 Ensure 'Turn on convenience PIN sign-in' is set to 'Disabled' (Automated)	781
18.9.29 Mitigation Options	783
18.9.30 Net Logon	783
18.9.31 OS Policies	783
18.9.32 PIN Complexity	783
18.9.33 Power Management	783
18.9.33.1 Button Settings	784
18.9.33.2 Energy Saver Settings	784
18.9.33.3 Hard Disk Settings	784
18.9.33.4 Notification Settings	784
18.9.33.5 Power Throttling Settings	784
18.9.33.6 Sleep Settings	785
18.9.33.6.1 Ensure 'Allow network connectivity during connected-standby (on battery)' is set to 'Disabled' (Automated)	786
18.9.33.6.2 Ensure 'Allow network connectivity during connected-standby (plugged in)' is set to 'Disabled' (Automated)	788
18.9.33.6.3 Ensure 'Require a password when a computer wakes (on battery)' is set to 'Enabled' (Automated)	790
18.9.33.6.4 Ensure 'Require a password when a computer wakes (plugged in)' is set to 'Enabled' (Automated)	792
18.9.34 Recovery	794
18.9.35 Remote Assistance	794
18.9.35.1 Ensure 'Configure Offer Remote Assistance' is set to 'Disabled' (Automated)	795
18.9.35.2 Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled' (Automated)	797
18.9.36 Remote Procedure Call	799

18.9.36.1 Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled' (MS only) (Automated)	800
18.9.36.2 Ensure 'Restrict Unauthenticated RPC clients' is set to 'Enabled: Authenticated' (MS only) (Automated)	802
18.9.37 Removable Storage Access	804
18.9.38 Scripts	804
18.9.39 Security Account Manager	804
18.9.40 Server Manager	804
18.9.41 Service Control Manager Settings.....	804
18.9.42 Shutdown	805
18.9.43 Shutdown Options	805
18.9.44 Storage Health	805
18.9.45 Storage Sense	805
18.9.46 System Restore	805
18.9.47 Troubleshooting and Diagnostics	806
18.9.47.1 Application Compatibility Diagnostics.....	806
18.9.47.2 Corrupted File Recovery.....	806
18.9.47.3 Disk Diagnostic.....	806
18.9.47.4 Fault Tolerant Heap	806
18.9.47.5 Microsoft Support Diagnostic Tool.....	806
18.9.47.5.1 Ensure 'Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider' is set to 'Disabled' (Automated).....	807
18.9.47.6 MSI Corrupted File Recovery	809
18.9.47.7 Scheduled Maintenance.....	809
18.9.47.8 Scripted Diagnostics	809
18.9.47.9 Windows Boot Performance Diagnostics	809
18.9.47.10 Windows Memory Leak Diagnosis	809
18.9.47.11 Windows Performance PerfTrack	810
18.9.47.11.1 Ensure 'Enable/Disable PerfTrack' is set to 'Disabled' (Automated)	811
18.9.48 Trusted Platform Module Services	813
18.9.49 User Profiles	813
18.9.49.1 Ensure 'Turn off the advertising ID' is set to 'Enabled' (Automated)	814
18.9.50 Windows File Protection	816
18.9.51 Windows Time Service	816
18.9.51.1 Time Providers.....	816
18.9.51.1.1 Ensure 'Enable Windows NTP Client' is set to 'Enabled' (Automated).....	817
18.9.51.1.2 Ensure 'Enable Windows NTP Client' is set to 'Enabled: DoD time server' (STIG only) (Automated)	819
18.9.51.1.3 Ensure 'Enable Windows NTP Server' is set to 'Disabled' (MS only) (Automated)	821
18.10 Windows Components	823
18.10.1 ActiveX Installer Service	823
18.10.2 Add features to Windows 10 (formerly Windows Anytime Upgrade)	823
18.10.3 App Package Deployment	823
18.10.3.1 Ensure 'Allow a Windows app to share application data between users' is set to 'Disabled' (Automated).....	824
18.10.4 App Privacy.....	826
18.10.5 App runtime	826
18.10.5.1 Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled' (Automated) ..	827
18.10.6 Application Compatibility	829
18.10.6.1 Ensure 'Turn off Inventory Collector' is set to 'Enabled' (STIG only) (Automated) ..	830
18.10.7 AutoPlay Policies	832
18.10.7.1 Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled' (Automated)	833
18.10.7.2 Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands' (Automated).....	835

18.10.7.3 Ensure 'Turn off Autoplay' is set to 'Enabled: All drives' (Automated)	837
18.10.8 Biometrics	839
18.10.8.1 Facial Features	839
18.10.8.1.1 Ensure 'Configure enhanced anti-spoofing' is set to 'Enabled' (Automated)	840
18.10.9 BitLocker Drive Encryption	842
18.10.10 Camera	842
18.10.10.1 Ensure 'Allow Use of Camera' is set to 'Disabled' (Automated)	843
18.10.11 Chat	845
18.10.12 Cloud Content	845
18.10.12.1 Ensure 'Turn off cloud consumer account state content' is set to 'Enabled' (Automated)	846
18.10.12.2 Ensure 'Turn off Microsoft consumer experiences' is set to 'Enabled' (Automated)	848
18.10.13 Connect	850
18.10.13.1 Ensure 'Require pin for pairing' is set to 'Enabled: First Time' OR 'Enabled: Always' (Automated)	851
18.10.14 Credential User Interface	853
18.10.14.1 Ensure 'Do not display the password reveal button' is set to 'Enabled' (Automated)	854
18.10.14.2 Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled' (Automated)	856
18.10.15 Data Collection and Preview Builds	858
18.10.15.1 Ensure 'Allow Diagnostic Data' is set to 'Enabled: Diagnostic data off (not recommended)' or 'Enabled: Send required diagnostic data' (Automated)	859
18.10.15.2 Ensure 'Configure Authenticated Proxy usage for the Connected User Experience and Telemetry service' is set to 'Enabled: Disable Authenticated Proxy usage' (Automated)	862
18.10.15.3 Ensure 'Disable OneSettings Downloads' is set to 'Enabled' (Automated)	864
18.10.15.4 Ensure 'Do not show feedback notifications' is set to 'Enabled' (Automated)	866
18.10.15.5 Ensure 'Enable OneSettings Auditing' is set to 'Enabled' (Automated)	868
18.10.15.6 Ensure 'Limit Diagnostic Log Collection' is set to 'Enabled' (Automated)	870
18.10.15.7 Ensure 'Limit Dump Collection' is set to 'Enabled' (Automated)	872
18.10.15.8 Ensure 'Toggle user control over Insider builds' is set to 'Disabled' (Automated)	874
18.10.16 Delivery Optimization	876
18.10.17 Desktop App Installer	876
18.10.18 Desktop Gadgets	876
18.10.19 Desktop Window Manager	876
18.10.20 Device and Driver Compatibility	876
18.10.21 Device Registration (formerly Workplace Join)	877
18.10.22 Digital Locker	877
18.10.23 Edge UI	877
18.10.24 Event Forwarding	877
18.10.25 Event Log Service	877
18.10.25.1 Application	878
18.10.25.1.1 Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated)	879
18.10.25.1.2 Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Automated)	881
18.10.25.2 Security	884
18.10.25.2.1 Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated)	885
18.10.25.2.2 Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater' (Automated)	887
18.10.25.3 Setup	889
18.10.25.3.1 Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated)	890

18.10.25.3.2 Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Automated)	892
18.10.25.4 System	894
18.10.25.4.1 Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated)	895
18.10.25.4.2 Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Automated)	897
18.10.26 Event Logging	899
18.10.27 Event Viewer	899
18.10.28 File Explorer (formerly Windows Explorer)	899
18.10.28.1 Previous Versions	899
18.10.28.2 Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled' (Automated)	900
18.10.28.3 Ensure 'Turn off heap termination on corruption' is set to 'Disabled' (Automated)	902
18.10.28.4 Ensure 'Turn off shell protocol protected mode' is set to 'Disabled' (Automated)	904
18.10.29 File History	906
18.10.30 Find My Device	906
18.10.31 Handwriting	906
18.10.32 HomeGroup	906
18.10.33 Human Presence	906
18.10.34 Internet Explorer	907
18.10.35 Internet Information Services	907
18.10.36 Location and Sensors	907
18.10.36.1 Ensure 'Turn off location' is set to 'Enabled' (Automated)	908
18.10.37 Maintenance Scheduler	910
18.10.38 Maps	910
18.10.39 MDM	910
18.10.40 Messaging	910
18.10.40.1 Ensure 'Allow Message Service Cloud Sync' is set to 'Disabled' (Automated)	911
18.10.41 Microsoft account	913
18.10.41.1 Ensure 'Block all consumer Microsoft account user authentication' is set to 'Enabled' (Automated)	914
18.10.42 Microsoft Defender Antivirus (formerly Windows Defender and Windows Defender Antivirus)	916
18.10.42.1 Client Interface	916
18.10.42.2 Device Control	916
18.10.42.3 Exclusions	916
18.10.42.4 Features	916
18.10.42.5 MAPS	917
18.10.42.5.1 Ensure 'Configure local setting override for reporting to Microsoft MAPS' is set to 'Disabled' (Automated)	918
18.10.42.5.2 Ensure 'Join Microsoft MAPS' is set to 'Disabled' (Automated)	920
18.10.42.6 Microsoft Defender Exploit Guard (formerly Windows Defender Exploit Guard)	923
18.10.42.6.1 Attack Surface Reduction	923
18.10.42.6.1.1 Ensure 'Configure Attack Surface Reduction rules' is set to 'Enabled' (Automated)	924
18.10.42.6.1.2 Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is configured (Automated)	926
18.10.42.6.2 Controlled Folder Access	929
18.10.42.6.3 Network Protection	929
18.10.42.6.3.1 Ensure 'Prevent users and apps from accessing dangerous websites' is set to 'Enabled: Block' (Automated)	930
18.10.42.7 MpEngine	932
18.10.42.7.1 Ensure 'Enable file hash computation feature' is set to 'Enabled' (Automated)	933
18.10.42.8 Network Inspection System	935

18.10.42.9 Quarantine	935
18.10.42.10 Real-time Protection	935
18.10.42.10.1 Ensure 'Scan all downloaded files and attachments' is set to 'Enabled' (Automated)	936
18.10.42.10.2 Ensure 'Turn off real-time protection' is set to 'Disabled' (Automated)	938
18.10.42.10.3 Ensure 'Turn on behavior monitoring' is set to 'Enabled' (Automated)	940
18.10.42.10.4 Ensure 'Turn on script scanning' is set to 'Enabled' (Automated)	942
18.10.42.11 Remediation	944
18.10.42.12 Reporting	944
18.10.42.12.1 Ensure 'Configure Watson events' is set to 'Disabled' (Automated)	945
18.10.42.13 Scan	947
18.10.42.13.1 Ensure 'Scan packed executables' is set to 'Enabled' (Automated)	948
18.10.42.13.2 Ensure 'Scan removable drives' is set to 'Enabled' (Automated)	950
18.10.42.13.3 Ensure 'Turn on e-mail scanning' is set to 'Enabled' (Automated)	952
18.10.42.14 Security Intelligence Updates (formerly Signature Updates)	954
18.10.42.15 Threats	954
18.10.42.16 Ensure 'Configure detection for potentially unwanted applications' is set to 'Enabled: Block' (Automated)	955
18.10.42.17 Ensure 'Turn off Microsoft Defender AntiVirus' is set to 'Disabled' (Automated)	957
18.10.43 Microsoft Defender Application Guard (formerly Windows Defender Application Guard)	959
18.10.44 Microsoft Defender Exploit Guard (formerly Windows Defender Exploit Guard)	959
18.10.45 Microsoft Edge	959
18.10.46 Microsoft Secondary Authentication Factor	960
18.10.47 Microsoft User Experience Virtualization	960
18.10.48 NetMeeting	960
18.10.49 News and interests	960
18.10.50 OneDrive (formerly SkyDrive)	960
18.10.50.1 Ensure 'Prevent the usage of OneDrive for file storage' is set to 'Enabled' (Automated)	961
18.10.51 Online Assistance	964
18.10.52 OOBE	964
18.10.53 Portable Operating System	964
18.10.54 Presentation Settings	964
18.10.55 Push To Install	964
18.10.55.1 Ensure 'Turn off Push To Install service' is set to 'Enabled' (Automated)	965
18.10.56 Remote Desktop Services (formerly Terminal Services)	967
18.10.56.1 RD Licensing (formerly TS Licensing)	967
18.10.56.2 Remote Desktop Connection Client	967
18.10.56.2.1 RemoteFX USB Device Redirection	967
18.10.56.2.2 Ensure 'Do not allow passwords to be saved' is set to 'Enabled' (Automated)	968
18.10.56.3 Remote Desktop Session Host (formerly Terminal Server)	970
18.10.56.3.1 Application Compatibility	970
18.10.56.3.2 Connections	970
18.10.56.3.2.1 Ensure 'Restrict Remote Desktop Services users to a single Remote Desktop Services session' is set to 'Enabled' (Automated)	971
18.10.56.3.3 Device and Resource Redirection	973
18.10.56.3.3.1 Ensure 'Do not allow COM port redirection' is set to 'Enabled' (Automated)	974
18.10.56.3.3.2 Ensure 'Do not allow drive redirection' is set to 'Enabled' (Automated)	976
18.10.56.3.3.3 Ensure 'Do not allow LPT port redirection' is set to 'Enabled' (Automated)	978
18.10.56.3.3.4 Ensure 'Do not allow supported Plug and Play device redirection' is set to 'Enabled' (Automated)	980
18.10.56.3.4 Licensing	982
18.10.56.3.5 Printer Redirection	982
18.10.56.3.6 Profiles	982
18.10.56.3.7 RD Connection Broker (formerly TS Connection Broker)	982

18.10.56.3.8 Remote Session Environment	982
18.10.56.3.9 Security	983
18.10.56.3.9.1 Ensure 'Always prompt for password upon connection' is set to 'Enabled' (Automated)	984
18.10.56.3.9.2 Ensure 'Require secure RPC communication' is set to 'Enabled' (Automated)	986
18.10.56.3.9.3 Ensure 'Require use of specific security layer for remote (RDP) connections' is set to 'Enabled: SSL' (Automated)	988
18.10.56.3.9.4 Ensure 'Require user authentication for remote connections by using Network Level Authentication' is set to 'Enabled' (Automated)	990
18.10.56.3.9.5 Ensure 'Set client connection encryption level' is set to 'Enabled: High Level' (Automated)	992
18.10.56.3.10 Session Time Limits	994
18.10.56.3.10.1 Ensure 'Set time limit for active but idle Remote Desktop Services sessions' is set to 'Enabled: 15 minutes or less, but not Never (0)' (Automated)	995
18.10.56.3.10.2 Ensure 'Set time limit for disconnected sessions' is set to 'Enabled: 1 minute' (Automated)	997
18.10.56.3.11 Temporary folders	999
18.10.56.3.11.1 Ensure 'Do not delete temp folders upon exit' is set to 'Disabled' (Automated)	1000
18.10.56.3.11.2 Ensure 'Do not use temporary folders per session' is set to 'Disabled' (Automated)	1002
18.10.57 RSS Feeds	1004
18.10.57.1 Ensure 'Prevent downloading of enclosures' is set to 'Enabled' (Automated)	1005
18.10.57.2 Ensure 'Turn on Basic feed authentication over HTTP' is set to 'Not configured' or 'Disabled' (STIG only) (Automated)	1007
18.10.58 Search	1009
18.10.58.1 OCR	1009
18.10.58.2 Ensure 'Allow Cloud Search' is set to 'Enabled: Disable Cloud Search' (Automated)	1010
18.10.58.3 Ensure 'Allow indexing of encrypted files' is set to 'Disabled' (Automated)	1012
18.10.58.4 Ensure 'Allow search highlights' is set to 'Disabled' (Automated)	1014
18.10.59 Security Center	1016
18.10.60 Shutdown Options	1016
18.10.61 Smart Card	1016
18.10.62 Software Protection Platform	1016
18.10.62.1 Ensure 'Turn off KMS Client Online AVS Validation' is set to 'Enabled' (Automated)	1017
18.10.63 Sound Recorder	1019
18.10.64 Speech	1019
18.10.65 Store	1019
18.10.66 Sync your settings	1019
18.10.67 Tablet PC	1019
18.10.68 Task Scheduler	1020
18.10.69 Tenant Restrictions	1020
18.10.70 Text Input	1020
18.10.71 Widgets	1020
18.10.72 Windows Calendar	1020
18.10.73 Windows Color System	1021
18.10.74 Windows Customer Experience Improvement Program	1021
18.10.75 Windows Defender SmartScreen	1021
18.10.75.1 Enhanced Phishing Protection	1021
18.10.75.2 Explorer	1021
18.10.75.2.1 Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled: Warn and prevent bypass' (Automated)	1022

18.10.75.2.2 Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled' (STIG only) (Automated)	1024
18.10.76 Windows Error Reporting.....	1027
18.10.77 Windows Game Recording and Broadcasting	1027
18.10.78 Windows Hello for Business (formerly Microsoft Passport for Work)	1027
18.10.79 Windows Ink Workspace	1027
18.10.79.1 Ensure 'Allow suggested apps in Windows Ink Workspace' is set to 'Disabled' (Automated)	1028
18.10.79.2 Ensure 'Allow Windows Ink Workspace' is set to 'Enabled: On, but disallow access above lock' OR 'Enabled: Disabled' (Automated)	1030
18.10.80 Windows Installer.....	1032
18.10.80.1 Ensure 'Allow user control over installs' is set to 'Disabled' (Automated).....	1033
18.10.80.2 Ensure 'Always install with elevated privileges' is set to 'Disabled' (Automated).....	1035
18.10.80.3 Ensure 'Prevent Internet Explorer security prompt for Windows Installer scripts' is set to 'Disabled' (Automated).....	1037
18.10.81 Windows Logon Options.....	1039
18.10.81.1 Ensure 'Sign-in and lock last interactive user automatically after a restart' is set to 'Disabled' (Automated).....	1040
18.10.82 Windows Media Digital Rights Management.....	1042
18.10.83 Windows Media Player	1042
18.10.84 Windows Messenger.....	1042
18.10.85 Windows Mobility Center	1042
18.10.86 Windows PowerShell	1042
18.10.86.1 Ensure 'Turn on PowerShell Script Block Logging' is set to 'Enabled' (Automated)	1043
18.10.86.2 Ensure 'Turn on PowerShell Transcription' is set to 'Enabled' (Automated)	1046
18.10.87 Windows Reliability Analysis.....	1048
18.10.88 Windows Remote Management (WinRM)	1048
18.10.88.1 WinRM Client.....	1048
18.10.88.1.1 Ensure 'Allow Basic authentication' is set to 'Disabled' (Automated)	1049
18.10.88.1.2 Ensure 'Allow unencrypted traffic' is set to 'Disabled' (Automated)	1051
18.10.88.1.3 Ensure 'Disallow Digest authentication' is set to 'Enabled' (Automated)	1053
18.10.88.2 WinRM Service.....	1055
18.10.88.2.1 Ensure 'Allow Basic authentication' is set to 'Disabled' (Automated)	1056
18.10.88.2.2 Ensure 'Allow remote server management through WinRM' is set to 'Disabled' (Automated)	1058
18.10.88.2.3 Ensure 'Allow unencrypted traffic' is set to 'Disabled' (Automated)	1060
18.10.88.2.4 Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled' (Automated)	1062
18.10.89 Windows Remote Shell.....	1064
18.10.89.1 Ensure 'Allow Remote Shell Access' is set to 'Disabled' (Automated)	1065
18.10.90 Windows Sandbox	1067
18.10.91 Windows Security (formerly Windows Defender Security Center)	1067
18.10.91.1 Account protection.....	1067
18.10.91.2 App and browser protection.....	1067
18.10.91.2.1 Ensure 'Prevent users from modifying settings' is set to 'Enabled' (Automated)	1068
18.10.92 Windows Update	1070
18.10.92.1 Legacy Policies.....	1070
18.10.92.1.1 Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled' (Automated).....	1071
18.10.92.2 Manage end user experience	1073
18.10.92.2.1 Ensure 'Configure Automatic Updates' is set to 'Enabled' (Automated).....	1074
18.10.92.2.2 Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day' (Automated).....	1076
18.10.92.3 Manage updates offered from Windows Server Update Service.....	1078

18.10.92.4 Manage updates offered from Windows Update (formerly Defer Windows Updates and Windows Update for Business)	1078
18.10.92.4.1 Ensure 'Manage preview builds' is set to 'Disabled' (Automated)	1079
18.10.92.4.2 Ensure 'Select when Preview Builds and Feature Updates are received' is set to 'Enabled: 180 or more days' (Automated)	1081
18.10.92.4.3 Ensure 'Select when Quality Updates are received' is set to 'Enabled: 0 days' (Automated)	1084
19 Administrative Templates (User)	1086
19.1 Control Panel.....	1086
19.2 Desktop	1086
19.3 Network.....	1086
19.4 Shared Folders	1086
19.5 Start Menu and Taskbar	1087
19.5.1 Notifications.....	1087
19.5.1.1 Ensure 'Turn off toast notifications on the lock screen' is set to 'Enabled' (Automated)	1088
19.6 System	1090
19.6.1 Ctrl+Alt+Del Options	1090
19.6.2 Display.....	1090
19.6.3 Driver Installation	1090
19.6.4 Folder Redirection.....	1090
19.6.5 Group Policy	1091
19.6.6 Internet Communication Management.....	1091
19.6.6.1 Internet Communication settings	1091
19.6.6.1.1 Ensure 'Turn off Help Experience Improvement Program' is set to 'Enabled' (Automated)	1092
19.7 Windows Components	1094
19.7.1 Account Notifications	1094
19.7.2 Add features to Windows 8 / 8.1 / 10 (formerly Windows Anytime Upgrade)	1094
19.7.3 App runtime	1094
19.7.4 Application Compatibility	1094
19.7.5 Attachment Manager.....	1095
19.7.5.1 Ensure 'Do not preserve zone information in file attachments' is set to 'Disabled' (Automated)	1096
19.7.5.2 Ensure 'Notify antivirus programs when opening attachments' is set to 'Enabled' (Automated)	1098
19.7.6 AutoPlay Policies	1100
19.7.7 Calculator	1100
19.7.8 Cloud Content.....	1100
19.7.8.1 Ensure 'Configure Windows spotlight on lock screen' is set to 'Disabled' (Automated)	1101
19.7.8.2 Ensure 'Do not suggest third-party content in Windows spotlight' is set to 'Enabled' (Automated)	1103
19.7.8.3 Ensure 'Do not use diagnostic data for tailored experiences' is set to 'Enabled' (Automated)	1105
19.7.8.4 Ensure 'Turn off all Windows spotlight features' is set to 'Enabled' (Automated)...	1107
19.7.8.5 Ensure 'Turn off Spotlight collection on Desktop' is set to 'Enabled' (Automated) ..	1109
19.7.9 Credential User Interface.....	1111
19.7.10 Data Collection and Preview Builds	1111
19.7.11 Desktop Gadgets.....	1111
19.7.12 Desktop Window Manager	1111
19.7.13 Digital Locker.....	1111
19.7.14 Edge UI	1112
19.7.15 File Explorer (formerly Windows Explorer)	1112
19.7.15.1 Explorer Frame Pane.....	1112

19.7.15.1.1 Ensure 'Turn off Preview Pane' is set to 'Enabled' (Automated)	1113
19.7.15.1.2 Ensure 'Turn on off details pane' is set to 'Enabled: Always hide' (Automated)	1115
19.7.16 File Revocation	1117
19.7.17 IME	1117
19.7.18 Instant Search.....	1117
19.7.19 Internet Explorer.....	1117
19.7.20 Location and Sensors.....	1117
19.7.21 Microsoft Edge	1118
19.7.22 Microsoft Management Console.....	1118
19.7.23 Microsoft User Experience Virtualization	1118
19.7.24 Multitasking	1118
19.7.25 NetMeeting	1118
19.7.26 Network Sharing.....	1119
19.7.26.1 Ensure 'Prevent users from sharing files within their profile.' is set to 'Enabled' (Automated)	1120
19.7.27 OOBE.....	1122
19.7.28 Presentation Settings	1122
19.7.29 Remote Desktop Services (formerly Terminal Services)	1122
19.7.30 RSS Feeds.....	1122
19.7.31 Search	1122
19.7.32 Sound Recorder	1123
19.7.33 Store	1123
19.7.34 Tablet PC.....	1123
19.7.35 Task Scheduler.....	1123
19.7.36 Windows Calendar	1123
19.7.37 Windows Color System	1124
19.7.38 Windows Copilot	1124
19.7.39 Windows Defender SmartScreen.....	1124
19.7.40 Windows Error Reporting.....	1124
19.7.41 Windows Hello for Business (formerly Microsoft Passport for Work)	1124
19.7.42 Windows Installer.....	1125
19.7.42.1 Ensure 'Always install with elevated privileges' is set to 'Disabled' (Automated) ..	1126
19.7.43 Windows Logon Options.....	1128
19.7.44 Windows Media Player	1128
19.7.44.1 Networking	1128
19.7.44.2 Playback	1128
19.7.44.2.1 Ensure 'Prevent Codec Download' is set to 'Enabled' (Automated)	1129
20 Additional Security Technical Implementation Guide (STIG) Settings	1131
20.1 Ensure 'Accounts require passwords' (Manual)	1132
20.2 Ensure 'Active Directory AdminSDHolder object is configured with proper audit settings' (STIG DC only) (Manual)	1134
20.3 Ensure 'Active Directory Domain Controllers Organizational Unit (OU) object have the proper access control permissions' (STIG DC only) (Manual)	1138
20.4 Ensure 'Active Directory Domain Controllers Organizational Unit (OU) object is configured with proper audit settings' (STIG DC only) (Manual)	1142
20.5 Ensure 'Active Directory Domain object is configured with proper audit settings' (STIG DC only) (Manual)	1146
20.6 Ensure 'Active Directory Group Policy objects are configured with proper audit settings' (STIG DC only) (Manual)	1150
20.7 Ensure 'Active Directory Group Policy objects have proper access control permissions' (STIG DC only) (Manual)	1154
20.8 Ensure 'Active Directory Infrastructure object is configured with proper audit settings' (STIG DC only) (Manual)	1157
20.9 Ensure 'Active Directory RID Manager\$ object is configured with proper audit settings' (STIG DC only) (Manual)	1161

20.10 Ensure 'Active Directory SYSVOL directory must have the proper access control permissions' (STIG DC only) (Manual)	1165
20.11 Ensure 'Active Directory user accounts are configured to require the use of a Common Access Card (CAC), Personal Identity Verification (PIV)-compliant hardware token, or Alternate Logon Token (ALT)' (STIG DC only) (Manual)	1169
20.12 Ensure 'Administrative accounts cannot be used with applications that access the Internet, such as web browsers, or with potential Internet sources, such as email' (Manual)	1171
20.13 Ensure 'Audit records must be backed up to a different system or media than the system being audited' (Manual)	1173
20.14 Ensure 'Automated mechanisms must be employed to determine the state of system components...' (Manual)	1175
20.15 Ensure 'Data files owned by users must be on a different logical partition from the directory server data files' (STIG DC only) (Manual)	1177
20.16 Ensure 'Default permissions for the HKEY_LOCAL_MACHINE registry hive must be maintained' (Manual)	1179
20.17 Ensure 'Deny-all, permit-by-exception policy to allow the execution of authorized software programs' (Manual)	1184
20.18 Ensure 'Directory data (outside the root DSE) of a non-public directory is configured' (STIG DC only) (Manual)	1187
20.19 Ensure 'Directory service must be configured to terminate LDAP-based network connections to the directory server after five minutes of inactivity' (STIG DC only) (Manual)	1190
20.20 Ensure 'DoD Interoperability Root CA cross-certificates' are installed in the 'Untrusted Certificates Store' on unclassified systems (Manual)	1192
20.21 Ensure 'DoD Root Certificate Authority (CA) certificates' are installed in the 'Trusted Root Store' (Manual)	1194
20.22 Ensure 'Domain Controller PKI certificates must be issued by the DoD PKI or an approved External Certificate Authority' (STIG DC only) (Manual)	1197
20.23 Ensure 'Domain controllers have a PKI server certificate' (STIG DC only) (Manual)	1199
20.24 Ensure 'Domain Controllers run on a machine dedicated to that function' (STIG DC only) (Manual)	1201
20.25 Ensure 'Domain-joined systems have a Trusted Platform Module (TPM) enabled and ready for use' (Manual)	1204
20.26 Ensure 'Emergency accounts must be automatically removed or disabled after the crisis is resolved or within 72 hours' (Manual)	1206
20.27 Ensure 'Event Viewer must be protected from unauthorized modification and deletion' (Manual)	1209
20.28 Ensure 'Fax Server role' is set to 'Not Installed' (Manual)	1211
20.29 Ensure 'FTP servers are configured to prevent access to the system drive' (Manual)	1213
20.30 Ensure 'FTP servers must be configured to prevent anonymous logons' (Manual)	1215
20.31 Ensure 'Host-based firewall is installed and enabled' (Manual)	1217
20.32 Ensure 'krbtgt account password' is no more than '180 days old' (STIG DC only) (Manual)	1219
20.33 Ensure 'Local volumes must use a format that supports NTFS attributes' (Manual)	1221
20.34 Ensure 'Manually managed application account passwords are 14 characters in length' (Manual)	1223
20.35 Ensure 'Manually managed application account passwords be changed at least annually or when a system administrator with knowledge of the password leaves the organization' (Manual)	1225
20.36 Ensure 'Members of the Backup Operators group have separate accounts for backup duties and normal operational tasks' (Manual)	1228
20.37 Ensure 'Non-administrative accounts or groups only have print permissions on printer shares' (Manual)	1230

20.38 Ensure 'Non-system-created file shares must limit access to groups that require it' (Manual)	1232
20.39 Ensure 'Off-load of audit records of interconnected systems in real time and off-load standalone systems weekly' (Manual)	1234
20.40 Ensure 'Only Administrators have Administrator rights on the system' (STIG MS only) (Manual)	1236
20.41 Ensure 'Only administrators responsible for the Domain Controller to have Administrator rights on the system' (STIG DC only) (Manual)	1239
20.42 Ensure 'Operating System is maintained at a supported servicing level' (Manual)	1241
20.43 Ensure 'Organization created Active Directory Organizational Unit (OU) objects have proper access control permissions' (STIG DC only) (Manual)	1243
20.44 Ensure 'Orphaned security identifiers (SIDs) must be removed from user rights' (Manual)	1247
20.45 Ensure 'Outdated or unused accounts are removed or disabled' (Manual)	1250
20.46 Ensure 'Passwords are configured to expire' (Manual)	1253
20.47 Ensure 'Permissions for program file directories must conform to minimum requirements' (Manual)	1255
20.48 Ensure 'Permissions for the Application Event Log must prevent access by non-privileged accounts' (Manual)	1259
20.49 Ensure 'Permissions for the Security Event Log must prevent access by non-privileged accounts' (Manual)	1261
20.50 Ensure 'Permissions for the System Event Log must prevent access by non-privileged accounts' (Manual)	1263
20.51 Ensure 'Permissions for the system drive root directory must conform to minimum requirements' (Manual)	1265
20.52 Ensure 'Permissions for the Windows installation directory conform to minimum requirements' (Manual)	1268
20.53 Ensure 'Permissions on Active Directory data files only allow System and Administrator access' (STIG DC only) (Manual)	1272
20.54 Ensure 'PKI certificates associated with user accounts must be issued by a DoD PKI or an approved External Certificate Authority (ECA)' (STIG DC only) (Manual)	1274
20.55 Ensure 'Protection methods such as TLS, encrypted VPN's, or IPsec must be implemented if the data owner has a strict requirement for ensuring data integrity and confidentiality is maintained at every step of the data transfer and handling process' (Manual)	1276
20.56 Ensure 'Separate NSA-approved (Type 1) cryptography is used' (STIG DC only) (Manual)	1278
20.57 Ensure 'Server Message Block (SMB) v1 protocol must not be installed' (Manual) ..	1280
20.58 Ensure 'Shared user accounts do not exist' (Manual)	1283
20.59 Ensure 'Software certificate installation files must be removed' (Manual)	1285
20.60 Ensure 'System files must be monitored for unauthorized changes' (Manual)	1287
20.61 Ensure 'Systems requiring data at rest protections must employ cryptographic mechanisms to prevent unauthorized disclosure and modification of the information at rest' (Manual)	1288
20.62 Ensure 'Telnet Client is not installed' (Manual)	1290
20.63 Ensure 'Temporary user accounts must be automatically removed or disabled after 72 hours' (Manual)	1292
20.64 Ensure 'TFTP Client' is 'not installed' (Manual)	1295
20.65 Ensure 'The system must have the Roles and Features required for it documented' (Manual)	1297
20.66 Ensure 'The system uses a host-based intrusion detection or prevention system' (Manual)	1299
20.67 Ensure 'The system uses an anti-virus program' (Manual)	1301
20.68 Ensure 'Unified Extensible Firmware Interface (UEFI) firmware must be configured and run in UEFI mode, not Legacy BIOS' (Manual)	1303

20.69 Ensure 'US DoD CCEB Interoperability Root CA cross-certificates' are installed in the 'Untrusted Certificates Store' on unclassified systems (Manual).....	1305
20.70 Ensure 'Users with Administrative privileges have separate accounts for administrative duties and normal operational tasks' (Manual)	1307
20.71 Ensure 'Windows PowerShell 2.0' is 'not installed' (Manual).....	1309
<i>Appendix: Summary Table</i>	<i>1311</i>
<i>Appendix: Change History</i>	<i>1371</i>

Overview

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

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

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

Important Usage Information

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

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

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

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

In addition, CIS has developed CIS [Build Kits](#) for some common technologies to assist in applying CIS Benchmarks™ Recommendations.

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

The following is a reasonable remediation approach to follow:

1. **NEVER** deploy a CIS Build Kit, or any internally developed remediation method, to production systems without proper testing.
2. Proper testing consists of the following:
 - a. Understand the configuration (including installed applications) of the targeted systems.
 - b. Read the Impact section of the given Recommendation to help determine if there might be an issue with the targeted systems.
 - c. Test the configuration changes on representative lab system(s). This way if there is some issue it can be resolved prior to deploying to any production systems.
 - d. When confident, initially deploy to a small sub-set of users and monitor closely for issues. This way if there is some issue it can be resolved prior to deploying more broadly.
 - e. When confident, iteratively deploy to additional groups and monitor closely for issues until deployment is complete. This way if there is some issue it can be resolved prior to continuing deployment.

NOTE: CIS and the CIS Benchmarks™ development communities in CIS WorkBench do their best to test and have high confidence in the Recommendations, but they cannot test potential conflicts with all possible system deployments. Known potential issues identified during CIS Benchmarks™ development are documented in the Impact section of each Recommendation.

By using CIS and/or CIS Benchmarks™ Certified tools, and being careful with remediation deployment, it is possible to harden large numbers of deployed systems in a cost effective, efficient, and safe manner.

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

CIS-CAT® Pro is also available to CIS [SecureSuite®](#) members.

Target Technology Details

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

This secure configuration guide is based on **Microsoft Windows Server 2016 Security Technical Implementation Guide (STIG)** and is intended for all versions of the **Server 2016** operating system, including older versions. This secure configuration guide was tested against **Microsoft Windows Server 2016 Datacenter**.

To ensure all new and updated group policy objects (GPOs) are installed on the system, please download the newest version of the **ADMX/ADML** templates for **Windows 11**.

Templates can be downloaded from Microsoft at: [Download ADMX Templates for Windows 11 2023 Update \[23H2\] from Official Microsoft Download Center](#).

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

Intended Audience

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

Consensus Guidance

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

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

Typographical Conventions

The following typographical conventions are used throughout this guide:

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

Recommendation Definitions

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

Title

Concise description for the recommendation's intended configuration.

Assessment Status

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

Automated

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

Manual

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

Profile

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

Description

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

Rationale Statement

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

Impact Statement

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

Audit Procedure

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

Remediation Procedure

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

Default Value

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

References

Additional documentation relative to the recommendation.

CIS Critical Security Controls® (CIS Controls®)

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

Additional Information

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

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1 - Domain Controller**

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

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

- **Level 1 - Member Server**

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

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

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

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

- **Level 2 - Domain Controller**

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

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

- **Level 2 - Member Server**

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

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

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

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

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

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

- **STIG Domain Controller**

This profile includes recommendations from the DoD Microsoft Windows Server 2016 Security Technical Implementation Guide. Overlap of recommendations from the CIS Level 1, Level 2, and NextGeneration profiles are present. If any of the CIS Level 1, Level 2, and NextGeneration profiles are applied, changes will need to be made since there can be a difference in configurations from the STIG profile. Note: Configuration differences are stated in the description of the recommendation, if present.

Items in this profile exhibit one or more of the following characteristics:

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

- **STIG Member Server**

This profile includes recommendations from the DoD Microsoft Windows Server 2016 Security Technical Implementation Guide. Overlap of recommendations from the CIS Level 1, Level 2, and NextGeneration profiles are present. If any of the CIS Level 1, Level 2, and NextGeneration profiles are applied, changes will need to be made since there can be a difference in configurations from the STIG profile. Note: Configuration differences are stated in the description of the recommendation, if present.

Items in this profile exhibit one or more of the following characteristics:

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

Acknowledgements

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

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

Editor

Haemish Edgerton
Jennifer Jarose

Contributor

Caleb Eifert
Aaron Margosis
Hardeep Mehrotara
Phil White
Matthew Woods
Kevin Zhang

Recommendations

1 Account Policies

This section contains recommendations for account policies.

1.1 Password Policy

This section contains recommendations for password policy.

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

Profile Applicability:

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

Description:

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

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

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

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

Rationale:

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

If you specify a low number for this policy setting, users will be able to use the same small number of passwords repeatedly. If you do not also configure the Minimum password age setting, users might repeatedly change their passwords until they can reuse their original password.

Impact:

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

Audit:

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

Remediation:

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

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

Default Value:

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

References:

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

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224869
Rule ID: SV-224869r569186_rule
STIG ID: WN16-AC-000040
Severity: CAT II

CIS Controls:

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

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

Profile Applicability:

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

Description:

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

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

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

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

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

Rationale:

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

Impact:

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

Audit:

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

Remediation:

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

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

Default Value:

42 days.

References:

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

CIS Controls:

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

1.1.3 Ensure 'Maximum password age' is set to '60 or fewer days, but not 0' (STIG only) (Automated)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

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

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

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

The recommended STIG state for this setting is **60 or fewer days, but not 0**.

Note: The CIS recommended state for this setting is: **365 or fewer days, but not 0**.

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:

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

Impact:

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

Audit:

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

Remediation:

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

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

Default Value:

42 days.

References:

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

Additional Information:

```
Microsoft Windows Server 2016 Security Technical Implementation Guide:  
Version 2, Release 8, Benchmark Date: May 15, 2024
```

```
Vul ID:    V-224870  
Rule ID:   SV-224870r569186_rule  
STIG ID:   WN16-AC-000050  
Severity:  CAT II
```

CIS Controls:

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

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

Profile Applicability:

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

Description:

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

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

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

Rationale:

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

Impact:

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

Audit:

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

Remediation:

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

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

Default Value:

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

References:

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

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224871
Rule ID: SV-224871r569186_rule
STIG ID: WN16-AC-000060
Severity: CAT II

CIS Controls:

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

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

Profile Applicability:

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

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.

Impact:

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

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

Audit:

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

Remediation:

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

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

Default Value:

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

References:

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

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224872
Rule ID: SV-224872r569186_rule
STIG ID: WN16-AC-000070
Severity: CAT II

CIS Controls:

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

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

Profile Applicability:

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

Description:

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

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

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

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

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

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

Rationale:

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

Impact:

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

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

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

Audit:

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

Remediation:

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

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

Default Value:

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

References:

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

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224873
Rule ID: SV-224873r569186_rule
STIG ID: WN16-AC-000080
Severity: CAT II

CIS Controls:

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

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

Profile Applicability:

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

Description:

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

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

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

Rationale:

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

Impact:

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

Audit:

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

Remediation:

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

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

Default Value:

Disabled.

References:

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

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224874
Rule ID: SV-224874r877397_rule
STIG ID: WN16-AC-000090
Severity: CAT II

CIS Controls:

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

1.2 Account Lockout Policy

This section contains recommendations for account lockout policy.

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

Profile Applicability:

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

Description:

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

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

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

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

Rationale:

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

Impact:

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

Audit:

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

Remediation:

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

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

Default Value:

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

References:

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

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224866
Rule ID: SV-224866r852301_rule
STIG ID: WN16-AC-000010
Severity: CAT II

CIS Controls:

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

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

Profile Applicability:

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

Description:

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

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

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

Rationale:

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

Impact:

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

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

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

Audit:

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

Remediation:

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

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

Default Value:

0 failed logon attempts.

References:

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

CIS Controls:

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

1.2.3 Ensure 'Account lockout threshold' is set to '3 or fewer invalid logon attempt(s), but not 0' (STIG only) (Automated)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

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

The recommended state for this setting is: **3 or fewer invalid logon attempt(s), but not 0**.

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

Rationale:

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

Impact:

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

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

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

Audit:

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

Remediation:

To establish the recommended configuration via GP, set the following UI path to **3 or fewer invalid login attempt(s), but not 0**:

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

Default Value:

0 failed logon attempts.

References:

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

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224867
Rule ID: SV-224867r569186_rule
STIG ID: WN16-AC-000020
Severity: CAT II

CIS Controls:

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

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

Profile Applicability:

- Level 1 - Member Server

Description:

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

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

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

Rationale:

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

Impact:

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

Audit:

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

Remediation:

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

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

Default Value:

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

References:

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

CIS Controls:

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

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

Profile Applicability:

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

Description:

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

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

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

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

Rationale:

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

Impact:

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

Audit:

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

Remediation:

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

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

Default Value:

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

References:

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

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224868
Rule ID: SV-224868r852302_rule
STIG ID: WN16-AC-000030
Severity: CAT II

CIS Controls:

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

1.3 Kerberos Policy

This section contains recommendations for Kerberos Policy.

1.3.1 Ensure 'Enforce user logon restrictions' is set to 'Enabled' (STIG DC only) (Manual)

Profile Applicability:

- STIG Domain Controller

Description:

This security setting determines whether the Kerberos V5 Key Distribution Center (KDC) validates every request for a session ticket against the user rights policy of the user account. Validation of each request for a session ticket is optional, because the extra step takes time and it may slow network access to services.

The STIG recommended state for this setting is: **Enabled**.

Rationale:

If this policy setting is disabled, users might be granted session tickets for services that they do not have the right to use.

Impact:

None - this is the default behavior.

Audit:

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

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Account Policy\Kerberos Policy\Enforce user logon restrictions
```

Default Value:

Enabled.

Additional Information:

```
Microsoft Windows Server 2016 Security Technical Implementation Guide:  
Version 2, Release 8, Benchmark Date: May 15, 2024
```

```
Vul ID:    V-224965  
Rule ID:   SV-224965r852340_rule  
STIG ID:   WN16-DC-000020  
Severity:  CAT II
```


1.3.2 Ensure 'Maximum lifetime for service ticket' is set to '600 or fewer minutes, but not 0' (STIG DC only) (Manual)

Profile Applicability:

- STIG Domain Controller

Description:

This security setting determines the maximum amount of time (in minutes) that a granted session ticket can be used to access a particular service. The setting must be greater than 10 minutes and less than or equal to the setting for Maximum lifetime for user ticket.

The STIG recommended state for this setting is: **600 or fewer minutes, but not 0.**

Rationale:

If a client presents an expired session ticket when it requests a connection to a server, the server returns an error message. The client must request a new session ticket from the Kerberos V5 Key Distribution Center (KDC). Once a connection is authenticated, however, it no longer matters whether the session ticket remains valid. Session tickets are used only to authenticate new connections with servers. Ongoing operations are not interrupted if the session ticket that is used to authenticate the connection expires during the connection.

Impact:

None - this is the default behavior.

Note: If you configure the value for the Maximum lifetime for service ticket setting too high, users might be able to access network resources outside of their logon hours. Also, users whose accounts were disabled might continue to have access to network services with valid service tickets that were issued before their accounts were disabled.

Audit:

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

Remediation:

To establish the recommended configuration via GP, set the following UI path to **600 or fewer minutes, but not 0**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Account  
Policy\Kerberos Policy\Maximum lifetime for service ticket
```

Default Value:

600 minutes.

Additional Information:

```
Microsoft Windows Server 2016 Security Technical Implementation Guide:  
Version 2, Release 8, Benchmark Date: May 15, 2024
```

```
Vul ID:    V-224966  
Rule ID:   SV-224966r852341_rule  
STIG ID:   WN16-DC-000030  
Severity:  CAT II
```

1.3.3 Ensure 'Maximum lifetime for user ticket' is set to '10 or fewer hours, but not 0' (STIG DC only) (Manual)

Profile Applicability:

- STIG Domain Controller

Description:

This security setting determines the maximum amount of time (in hours) that a user's ticket-granting ticket (TGT) may be used.

The STIG recommended state for this setting is: **10 or fewer hours, but not 0**.

Rationale:

If you configure the value for the Maximum lifetime for user ticket setting too high, users might be able to access network resources outside of their logon hours. Also, users whose accounts were disabled might continue to have access to network services with valid user tickets that were issued before their accounts were disabled. If you configure this value too low, ticket requests to the KDC may affect the performance of your KDC and present an opportunity for a DoS attack.

Impact:

None - this is the default behavior.

Audit:

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

Remediation:

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

Computer Configuration\Policies\Windows Settings\Security Settings\Account Policy\Kerberos Policy\Maximum lifetime for user ticket

Default Value:

10 hours

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224967
Rule ID: SV-224967r852342_rule
STIG ID: WN16-DC-000040
Severity: CAT II

1.3.4 Ensure 'Maximum lifetime for user ticket renewal' is set to '7 or fewer days' (STIG DC only) (Manual)

Profile Applicability:

- STIG Domain Controller

Description:

This security setting determines the period of time (in days) during which a user's ticket-granting ticket can be renewed.

The STIG recommended state for this setting is: **7 or fewer days**.

Rationale:

If the value for this policy setting is too high, users may be able to renew very old user ticket-granting tickets. If the value is 0, ticket-granting tickets never expire.

Impact:

None - this is the default behavior.

Audit:

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

Remediation:

To establish the recommended configuration via GP, set the following UI path to **7 or fewer days**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Account Policy\Kerberos Policy\Maximum lifetime for user ticket renewal
```

Default Value:

7 days

Additional Information:

```
Microsoft Windows Server 2016 Security Technical Implementation Guide:  
Version 2, Release 8, Benchmark Date: May 15, 2024
```

```
Vul ID: V-224968  
Rule ID: SV-224968r852343_rule  
STIG ID: WN16-DC-000050  
Severity: CAT II
```

1.3.5 Ensure 'Maximum tolerance for computer clock synchronization' is set to '5 or fewer minutes' (STIG DC only) (Manual)

Profile Applicability:

- STIG Domain Controller

Description:

This security setting determines the maximum time difference (in minutes) that Kerberos V5 tolerates between the time on the client clock and the time on the domain controller that provides Kerberos authentication.

The STIG recommended state for this setting is: **5 or fewer minutes**.

Rationale:

To prevent replay attacks, the Kerberos v5 protocol uses time stamps as part of its protocol definition. For time stamps to work properly, the clocks of the client and the domain controller need to be in sync as much as possible. In other words, both devices must be set to the same time and date. Because the clocks of two computers are often out of sync, you can use this policy setting to establish the maximum acceptable difference to the Kerberos protocol between a client clock and domain controller clock. If the difference between a client computer clock and the domain controller clock is less than the maximum time difference that is specified in this policy, any time stamp that is used in a session between the two devices is considered to be authentic.

Impact:

None - this is the default behavior.

Audit:

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

Remediation:

To establish the recommended configuration via GP, set the following UI path to **5 or fewer minutes**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Account Policy\Kerberos Policy\Maximum tolerance for computer clock synchronization
```

Default Value:

5 minutes

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224969
Rule ID: SV-224969r852344_rule
STIG ID: WN16-DC-000060
Severity: CAT II

2 Local Policies

This section contains recommendations for local policies.

2.1 Audit Policy

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

2.2 User Rights Assignment

This section contains recommendations for user rights assignments.

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

Profile Applicability:

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

Description:

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

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

Rationale:

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

Impact:

None - this is the default behavior.

Audit:

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

Remediation:

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

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

Default Value:

No one.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225070
Rule ID: SV-225070r877392_rule
STIG ID: WN16-UR-000010
Severity: CAT II

CIS Controls:

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

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

Profile Applicability:

- Level 1 - Domain Controller
- STIG Domain Controller

Description:

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

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

Rationale:

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

Impact:

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

Audit:

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

Remediation:

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

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

Default Value:

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

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224997
Rule ID: SV-224997r569186_rule
STIG ID: WN16-DC-000340
Severity: CAT II

CIS Controls:

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

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

Profile Applicability:

- Level 1 - Member Server
- STIG Member Server

Description:

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

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

Rationale:

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

Impact:

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

Audit:

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

Remediation:

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

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

Default Value:

Administrators, Backup Operators, Users, Everyone.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225014
Rule ID: SV-225014r857272_rule
STIG ID: WN16-MS-000340
Severity: CAT II

CIS Controls:

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

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

Profile Applicability:

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

Description:

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

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

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

Rationale:

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

Impact:

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

Audit:

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

Remediation:

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

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

Default Value:

No one.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225071
Rule ID: SV-225071r877392_rule
STIG ID: WN16-UR-000030
Severity: CAT I

CIS Controls:

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

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

Profile Applicability:

- Level 1 - Domain Controller
- STIG Domain Controller

Description:

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

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

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

Rationale:

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

Impact:

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

Audit:

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

Remediation:

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

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

Default Value:

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

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224998
Rule ID: SV-224998r877392_rule
STIG ID: WN16-DC-000350
Severity: CAT II

CIS Controls:

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

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

Profile Applicability:

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

Description:

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

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

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

Note #2: A Member Server with Microsoft SQL Server installed will require a special exception to this recommendation for additional SQL-generated entries to be granted this user right.

Rationale:

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

Impact:

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

Audit:

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

Remediation:

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

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

Default Value:

Administrators, LOCAL SERVICE, NETWORK SERVICE.

CIS Controls:

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

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

Profile Applicability:

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

Description:

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

The recommended state for this setting is: **Administrators, ENTERPRISE DOMAIN CONTROLLERS**.

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

Note #2: When a server is promoted to a Domain Controller **ENTERPRISE DOMAIN CONTROLLERS** is granted this user right by default.

Rationale:

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

Impact:

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

Audit:

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

Remediation:

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

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

Default Value:

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

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225072
Rule ID: SV-225072r569186_rule
STIG ID: WN16-UR-000050
Severity: CAT II

CIS Controls:

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

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

Profile Applicability:

- Level 1 - Domain Controller
- STIG Domain Controller

Description:

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

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

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

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

Note #2: The above lists are to be treated as whitelists, which implies that the above principals need not be present for assessment of this recommendation to pass.

Note #3: In all versions of Windows Server prior to Server 2008 R2, **Remote Desktop Services** was known as **Terminal Services**, so you should substitute the older term if comparing against an older OS.

Rationale:

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

Impact:

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

Audit:

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

Remediation:

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

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

Default Value:

Administrators.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224999
Rule ID: SV-224999r569186_rule
STIG ID: WN16-DC-000360
Severity: CAT II

CIS Controls:

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

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

Profile Applicability:

- Level 1 - Member Server

Description:

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

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

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

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

Note #2: The above lists are to be treated as whitelists, which implies that the above principals need not be present for assessment of this recommendation to pass.

Note #3: In all versions of Windows Server prior to Server 2008 R2, **Remote Desktop Services** was known as **Terminal Services**, so you should substitute the older term if comparing against an older OS.

Rationale:

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

Impact:

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

Audit:

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

Remediation:

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

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

Default Value:

Administrators, Remote Desktop Users.

CIS Controls:

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

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

Profile Applicability:

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

Description:

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

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

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

Rationale:

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

Impact:

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

Audit:

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

Remediation:

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

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

Default Value:

On Member Servers: Administrators, Backup Operators.

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

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225073
Rule ID: SV-225073r877392_rule
STIG ID: WN16-UR-000070
Severity: CAT II

CIS Controls:

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

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

Profile Applicability:

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

Description:

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

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

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

Rationale:

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

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

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

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

Impact:

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

Audit:

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

Remediation:

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

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

Default Value:

On Member Servers: Administrators, LOCAL SERVICE.

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

CIS Controls:

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

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

Profile Applicability:

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

Description:

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

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

Rationale:

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

Impact:

None - this is the default behavior.

Audit:

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

Remediation:

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

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

Default Value:

Administrators, LOCAL SERVICE.

CIS Controls:

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

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

Profile Applicability:

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

Description:

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

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

Rationale:

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

Impact:

None - this is the default behavior.

Audit:

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

Remediation:

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

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

Default Value:

Administrators.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225074
Rule ID: SV-225074r877392_rule
STIG ID: WN16-UR-000080
Severity: CAT II

CIS Controls:

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

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

Profile Applicability:

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

Description:

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

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

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

Rationale:

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

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

Impact:

None - this is the default behavior.

Audit:

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

Remediation:

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

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

Default Value:

No one.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225091
Rule ID: SV-225091r877392_rule
STIG ID: WN16-UR-000090
Severity: CAT I

CIS Controls:

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

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

Profile Applicability:

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

Description:

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

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

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

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

Rationale:

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

Impact:

None - this is the default behavior.

Audit:

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

Remediation:

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

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

Default Value:

Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225076
Rule ID: SV-225076r877392_rule
STIG ID: WN16-UR-000100
Severity: CAT II

CIS Controls:

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

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

Profile Applicability:

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

Description:

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

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

Rationale:

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

Impact:

None - this is the default behavior.

Audit:

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

Remediation:

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

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

Default Value:

No one.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225077
Rule ID: SV-225077r877392_rule
STIG ID: WN16-UR-000110
Severity: CAT II

CIS Controls:

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

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

Profile Applicability:

- Level 1 - Domain Controller

Description:

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

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

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

Rationale:

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

Impact:

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

Audit:

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

Remediation:

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

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

Default Value:

Administrators.

CIS Controls:

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

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

Profile Applicability:

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

Description:

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

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

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

Rationale:

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

Impact:

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

Audit:

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

Remediation:

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

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

Default Value:

Administrators.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225078
Rule ID: SV-225078r877392_rule
STIG ID: WN16-UR-000120
Severity: CAT II

CIS Controls:

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

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

Profile Applicability:

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

Description:

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

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

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

Rationale:

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

Impact:

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

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

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

Audit:

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

Remediation:

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

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

Default Value:

Administrators.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225079
Rule ID: SV-225079r877392_rule
STIG ID: WN16-UR-000130
Severity: CAT I

CIS Controls:

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

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

Profile Applicability:

- Level 1 - Domain Controller
- STIG Domain Controller

Description:

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

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

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

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

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

Rationale:

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

Impact:

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

Audit:

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

Remediation:

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

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

Default Value:

Guest.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225000
Rule ID: SV-225000r569186_rule
STIG ID: WN16-DC-000370
Severity: CAT II

CIS Controls:

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

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

Profile Applicability:

- Level 1 - Member Server

Description:

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

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

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

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

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

Rationale:

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

Impact:

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

Audit:

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

Remediation:

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

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

Default Value:

No one.

CIS Controls:

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

2.2.22 Ensure 'Deny access to this computer from the network' to include 'Guests, Enterprise Admins Group, Domains Admins Group, Local account, and member of Administrators group' (STIG MS only) (Automated)

Profile Applicability:

- STIG Member Server

Description:

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

The recommended STIG state for this setting is to include: **Guests, Enterprise Admins Group, Domains Admins Group, Local account, and member of Administrators group**.

Note: The CIS recommended state for this setting is: **Guests, Local account, and member of Administrators group**, which differs from the STIG recommended state.

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

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

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

Rationale:

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

Impact:

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

Audit:

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

Remediation:

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

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

Default Value:

No one.

Additional Information:

```
Microsoft Windows Server 2016 Security Technical Implementation Guide:  
Version 2, Release 8, Benchmark Date: May 15, 2024
```

```
Vul ID:    V-225015  
Rule ID:   SV-225015r857274_rule  
STIG ID:   WN16-MS-000370  
Severity:  CAT II
```

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

Profile Applicability:

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

Description:

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

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

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

Rationale:

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

Impact:

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

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

Audit:

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

Remediation:

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

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

Default Value:

No one.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225001
Rule ID: SV-225001r569186_rule
STIG ID: WN16-DC-000380
Severity: CAT II

CIS Controls:

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

2.2.24 Ensure 'Deny log on as a batch job' to include 'Guests, Enterprise Admins Group, and Domain Admins Group' (STIG MS only) (Automated)

Profile Applicability:

- STIG Member Server

Description:

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

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

The recommended STIG state for this setting is to include: **Guests, Enterprise Admins Group, and Domain Admins Group**.

Note: The CIS recommended state for this setting is: **Guests** for both Domain Controllers and Member Servers, which differs from the STIG recommended state.

Rationale:

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

Impact:

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

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

Audit:

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

Remediation:

To establish the recommended configuration via GP, set the following UI path to include **Guests, Enterprise Admins Group, and Domain Admins Group**:

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

Default Value:

No one.

Additional Information:

```
Microsoft Windows Server 2016 Security Technical Implementation Guide:  
Version 2, Release 8, Benchmark Date: May 15, 2024
```

```
Vul ID:    V-225016  
Rule ID:   SV-225016r857276_rule  
STIG ID:   WN16-MS-000380  
Severity:  CAT II
```

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

Profile Applicability:

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

Description:

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

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

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

Rationale:

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

Impact:

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

Audit:

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

Remediation:

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

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

Default Value:

No one.

CIS Controls:

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

2.2.26 Ensure 'Deny log on as a service' to include 'No one' (STIG DC only) (Automated)

Profile Applicability:

- STIG Domain Controller

Description:

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

The recommended STIG state for this setting is to include: **No one**.

Note: The CIS recommended state for this setting is: **Guests** for both Domain Controllers and Member Servers, which differs from the STIG recommended state.

Note #2: This security setting does not apply to the **System**, **Local Service**, or **Network Service** accounts.

Rationale:

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

Impact:

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

Audit:

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

Remediation:

To establish the recommended configuration via GP, set the following UI path to include **No one**:

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

Default Value:

No one.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225002
Rule ID: SV-225002r569186_rule
STIG ID: WN16-DC-000390
Severity: CAT II

2.2.27 Ensure 'Deny log on as a service' to include 'Enterprise Admins Group and Domain Admins Group' (STIG MS only) (Automated)

Profile Applicability:

- STIG Member Server

Description:

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

The recommended STIG state for this setting is to include: **Enterprise Admins Group and Domain Admins Group**.

Note: The CIS recommended state for this setting is: **Guests** for both Domain Controllers and Member Servers, which differs from the STIG recommended state.

Note #2: This security setting does not apply to the **System, Local Service, or Network Service** accounts.

Rationale:

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

Impact:

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

Audit:

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

Remediation:

To establish the recommended configuration via GP, set the following UI path to include **Enterprise Admins Group and Domain Admins Group**:

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

Default Value:

No one.

Additional Information:

```
Microsoft Windows Server 2016 Security Technical Implementation Guide:  
Version 2, Release 8, Benchmark Date: May 15, 2024
```

```
Vul ID:    V-225017  
Rule ID:   SV-225017r890505_rule  
STIG ID:   WN16-MS-000390  
Severity:  CAT II
```

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

Profile Applicability:

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

Description:

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

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

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

Rationale:

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

Impact:

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

Audit:

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

Remediation:

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

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

Default Value:

No one.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225003
Rule ID: SV-225003r569186_rule
STIG ID: WN16-DC-000400
Severity: CAT II

CIS Controls:

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

2.2.29 Ensure 'Deny log on locally' to include 'Guests, Enterprise Admins group, and Domain Admins group' (STIG MS only) (Automated)

Profile Applicability:

- STIG Member Server

Description:

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

The recommended state for this setting is to include: **Guests, Enterprise Admins group, and Domain Admins group**.

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

Note: The CIS recommended state for this setting is: **Guests**, which differs from the STIG recommended state.

Rationale:

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

Impact:

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

Audit:

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

Remediation:

To establish the recommended configuration via GP, set the following UI path to include **Guests, Enterprise Admins group, and Domain Admins group**:

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

Default Value:

No one.

Additional Information:

```
Microsoft Windows Server 2016 Security Technical Implementation Guide:  
Version 2, Release 8, Benchmark Date: May 15, 2024
```

```
Vul ID:    V-225018  
Rule ID:   SV-225018r857278_rule  
STIG ID:   WN16-MS-000400  
Severity:  CAT II
```

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

Profile Applicability:

- Level 1 - Domain Controller
- STIG Domain Controller

Description:

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

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

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

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

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

Rationale:

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

Impact:

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

Audit:

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

Remediation:

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

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

Default Value:

No one.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225004
Rule ID: SV-225004r852366_rule
STIG ID: WN16-DC-000410
Severity: CAT II

CIS Controls:

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

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

Profile Applicability:

- Level 1 - Member Server

Description:

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

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

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

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

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

Rationale:

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

Impact:

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

Audit:

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

Remediation:

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

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

Default Value:

No one.

CIS Controls:

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

2.2.32 Ensure 'Deny log on through Remote Desktop Services' is set to 'Guests, Local account, Enterprise Admins Group, and Domain Admins Group' (STIG MS only) (Automated)

Profile Applicability:

- STIG Member Server

Description:

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

The recommended STIG state for this setting is: **Guests, Local account, Enterprise Admins Group, and Domain Admins Group**.

Note: The CIS recommended state for this setting is: **Guests and Local account**, which differs from the STIG recommended state.

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

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

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

Rationale:

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

Impact:

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

Audit:

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

Remediation:

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

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

Default Value:

No one.

Additional Information:

```
Microsoft Windows Server 2016 Security Technical Implementation Guide:  
Version 2, Release 8, Benchmark Date: May 15, 2024
```

```
Vul ID:    V-225019  
Rule ID:   SV-225019r860023_rule  
STIG ID:   WN16-MS-000410  
Severity:  CAT II
```

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

Profile Applicability:

- Level 1 - Domain Controller
- STIG Domain Controller

Description:

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

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

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

Rationale:

Misuse of the **Enable computer and user accounts to be trusted for delegation** user right could allow unauthorized users to impersonate other users on the network. An attacker could exploit this privilege to gain access to network resources and make it difficult to determine what has happened after a security incident.

Impact:

None - this is the default behavior.

Audit:

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

Remediation:

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

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

Default Value:

Administrators.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225005
Rule ID: SV-225005r877392_rule
STIG ID: WN16-DC-000420
Severity: CAT II

CIS Controls:

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

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

Profile Applicability:

- Level 1 - Member Server
- STIG Member Server

Description:

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

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

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

Rationale:

Misuse of the **Enable computer and user accounts to be trusted for delegation** user right could allow unauthorized users to impersonate other users on the network. An attacker could exploit this privilege to gain access to network resources and make it difficult to determine what has happened after a security incident.

Impact:

None - this is the default behavior.

Audit:

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

Remediation:

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

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

Default Value:

No one.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225020
Rule ID: SV-225020r877392_rule
STIG ID: WN16-MS-000420
Severity: CAT II

CIS Controls:

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

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

Profile Applicability:

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

Description:

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

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

Rationale:

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

Impact:

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

Audit:

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

Remediation:

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

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

Default Value:

On Member Servers: Administrators.

On Domain Controllers: Administrators, Server Operators.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225080
Rule ID: SV-225080r877392_rule
STIG ID: WN16-UR-000200
Severity: CAT II

CIS Controls:

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

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

Profile Applicability:

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

Description:

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

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

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

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

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

Rationale:

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

Impact:

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

Audit:

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

Remediation:

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

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

Default Value:

LOCAL SERVICE, NETWORK SERVICE.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225081
Rule ID: SV-225081r877392_rule
STIG ID: WN16-UR-000210
Severity: CAT II

CIS Controls:

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

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

Profile Applicability:

- Level 1 - Domain Controller
- STIG Domain Controller

Description:

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

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

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

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

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

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

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

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

Rationale:

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

Impact:

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

Audit:

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

Remediation:

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

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

Default Value:

Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225082
Rule ID: SV-225082r877392_rule
STIG ID: WN16-UR-000220
Severity: CAT II

CIS Controls:

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

2.2.38 Ensure 'Impersonate a client after authentication' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' and (when the Web Server (IIS) Role with Web Services Role Service is installed) 'IIS_IUSRS' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

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

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

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

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

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

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

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

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

Rationale:

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

Impact:

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

Audit:

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

Remediation:

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

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

Default Value:

Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE.

CIS Controls:

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

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

Profile Applicability:

- STIG Member Server

Description:

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

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

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

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

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

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

Note: The CIS recommended state for this setting is: **Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE** and (when the *Web Server (IIS)* Role with *Web Services* Role Service is installed) **IIS_IUSRS** (MS), which differs from the STIG recommended state.

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

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

Rationale:

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

Impact:

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

Audit:

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

Remediation:

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

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

Default Value:

Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225082
Rule ID: SV-225082r877392_rule
STIG ID: WN16-UR-000220
Severity: CAT II

2.2.40 Ensure 'Increase scheduling priority' is set to 'Administrators' (Automated)

Profile Applicability:

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

Description:

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

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

Rationale:

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

Impact:

None - this is the default behavior.

Audit:

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

Remediation:

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

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

Default Value:

On Windows Server 2016 or older: Administrators.

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

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225083
Rule ID: SV-225083r877392_rule
STIG ID: WN16-UR-000230
Severity: CAT II

CIS Controls:

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

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

Profile Applicability:

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

Description:

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

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

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

Rationale:

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

Impact:

If you remove the **Load and unload device drivers** user right from the **Print Operators** group or other accounts you could limit the abilities of users who are assigned to specific administrative roles in your environment. You should ensure that delegated tasks will not be negatively affected.

Audit:

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

Remediation:

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

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

Default Value:

On Member Servers: Administrators.

On Domain Controllers: Administrators, Print Operators.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225084
Rule ID: SV-225084r877392_rule
STIG ID: WN16-UR-000240
Severity: CAT II

CIS Controls:

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

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

Profile Applicability:

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

Description:

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

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

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

Rationale:

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

Impact:

None - this is the default behavior.

Audit:

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

Remediation:

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

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

Default Value:

No one.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225085
Rule ID: SV-225085r877392_rule
STIG ID: WN16-UR-000250
Severity: CAT II

CIS Controls:

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

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

Profile Applicability:

- Level 2 - Domain Controller

Description:

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

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

Rationale:

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

Impact:

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

Audit:

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

Remediation:

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

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

Default Value:

Administrators, Backup Operators.

CIS Controls:

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

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

Profile Applicability:

- Level 1 - Domain Controller

Description:

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

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

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

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

Rationale:

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

Impact:

None - this is the default behavior.

Audit:

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

Remediation:

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

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

Default Value:

Administrators.

CIS Controls:

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

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

Profile Applicability:

- Level 1 - Member Server
- STIG Member Server

Description:

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

For environments running Microsoft Exchange Server, the **Exchange Servers** group must possess this privilege on Domain Controllers to properly function. Given this, DCs that grant the **Exchange Servers** group this privilege also conform to this benchmark. If the environment does not use Microsoft Exchange Server, then this privilege should be limited to only **Administrators** on DCs.

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

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

Rationale:

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

Impact:

None - this is the default behavior.

Audit:

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

Remediation:

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

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

Default Value:

Administrators.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225086
Rule ID: SV-225086r569186_rule
STIG ID: WN16-UR-000260
Severity: CAT II

CIS Controls:

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

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

Profile Applicability:

- STIG Domain Controller

Description:

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

For environments running Microsoft Exchange Server, the **Exchange Servers** group must possess this privilege on Domain Controllers to properly function. Given this, DCs that grant the **Exchange Servers** group this privilege also conform to this benchmark. If the environment does not use Microsoft Exchange Server, then this privilege should be limited to only **Administrators** on DCs.

The recommended STIG state for this setting is: **Administrators**.

Note: The CIS recommended state for this setting is: **Administrators** and (when Exchange is running in the environment) **Exchange Servers**, which differs from the STIG recommended state.

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

Rationale:

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

Impact:

None - this is the default behavior.

Audit:

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

Remediation:

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

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

Default Value:

Administrators.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225086
Rule ID: SV-225086r852405_rule
STIG ID: WN16-UR-000260
Severity: CAT II

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

Profile Applicability:

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

Description:

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

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

Rationale:

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

Impact:

None - this is the default behavior.

Audit:

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

Remediation:

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

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

Default Value:

No one.

CIS Controls:

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

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

Profile Applicability:

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

Description:

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

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

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

Rationale:

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

Impact:

None - this is the default behavior.

Audit:

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

Remediation:

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

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

Default Value:

Administrators.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225087
Rule ID: SV-225087r877392_rule
STIG ID: WN16-UR-000270
Severity: CAT II

CIS Controls:

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

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

Profile Applicability:

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

Description:

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

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

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

Rationale:

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

Impact:

None - this is the default behavior.

Audit:

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

Remediation:

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

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

Default Value:

Administrators.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225088
Rule ID: SV-225088r891712_rule
STIG ID: WN16-UR-000280
Severity: CAT II

CIS Controls:

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

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

Profile Applicability:

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

Description:

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

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

Rationale:

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

Impact:

None - this is the default behavior.

Audit:

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

Remediation:

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

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

Default Value:

Administrators.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225089
Rule ID: SV-225089r877392_rule
STIG ID: WN16-UR-000290
Severity: CAT II

CIS Controls:

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

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

Profile Applicability:

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

Description:

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

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

Rationale:

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

Impact:

None - this is the default behavior.

Audit:

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

Remediation:

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

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

Default Value:

Windows Server 2008 (non-R2): Administrators.

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

CIS Controls:

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

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

Profile Applicability:

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

Description:

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

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

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

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

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

Rationale:

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

Impact:

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

Audit:

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

Remediation:

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

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

Default Value:

LOCAL SERVICE, NETWORK SERVICE.

CIS Controls:

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

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

Profile Applicability:

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

Description:

This policy setting determines which users can bypass file, directory, registry, and other persistent object permissions when restoring backed up files and directories on computers that run Windows Vista (or newer) in your environment. This user right also determines which users can set valid security principals as object owners; it is similar to the **Back up files and directories** user right.

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

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

Rationale:

An attacker with the **Restore files and directories** user right could restore sensitive data to a computer and overwrite data that is more recent, which could lead to loss of important data, data corruption, or a denial of service. Attackers could overwrite executable files that are used by legitimate administrators or system services with versions that include malicious software to grant themselves elevated privileges, compromise data, or install backdoors for continued access to the computer.

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

Impact:

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

Audit:

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

Remediation:

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

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

Default Value:

On Member Servers: Administrators, Backup Operators.

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

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225092
Rule ID: SV-225092r877392_rule
STIG ID: WN16-UR-000300
Severity: CAT II

CIS Controls:

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

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

Profile Applicability:

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

Description:

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

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

Rationale:

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

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

Impact:

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

Audit:

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

Remediation:

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

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

Default Value:

On Member Servers: Administrators, Backup Operators.

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

CIS Controls:

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

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

Profile Applicability:

- Level 1 - Domain Controller

Description:

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

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

Rationale:

The **Synchronize directory service data** user right affects Domain Controllers; only Domain Controllers should be able to synchronize directory service data. Domain Controllers have this user right inherently, because the synchronization process runs in the context of the **System** account on Domain Controllers. Attackers who have this user right can view all information stored within the directory. They could then use some of that information to facilitate additional attacks or expose sensitive data, such as direct telephone numbers or physical addresses.

Impact:

None - this is the default behavior.

Audit:

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

Remediation:

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

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

Default Value:

No one.

CIS Controls:

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

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

Profile Applicability:

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

Description:

This policy setting allows users to take ownership of files, folders, registry keys, processes, or threads. This user right bypasses any permissions that are in place to protect objects to give ownership to the specified user.

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

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

Rationale:

Any users with the **Take ownership of files or other objects** user right can take control of any object, regardless of the permissions on that object, and then make any changes they wish to that object. Such changes could result in exposure of data, corruption of data, or a DoS condition.

Impact:

None - this is the default behavior.

Audit:

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

Remediation:

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

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

Default Value:

Administrators.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225093
Rule ID: SV-225093r877392_rule
STIG ID: WN16-UR-000310
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

2.3 Security Options

This section contains recommendations for security options.

2.3.1 Accounts

This section contains recommendations related to default accounts.

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

Profile Applicability:

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

Description:

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

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

Rationale:

Organizations that want to effectively implement identity management policies and maintain firm control of what accounts are used to log onto their computers will probably want to block Microsoft accounts. Organizations may also need to block Microsoft accounts in order to meet the requirements of compliance standards that apply to their information systems.

Impact:

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

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **3**.

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

Remediation:

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

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

Default Value:

Users are able to use Microsoft accounts with Windows.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.6 <u>Centralize Account Management</u> Centralize account management through a directory or identity service.			
v7	16.2 <u>Configure Centralized Point of Authentication</u> Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.			

2.3.1.2 Ensure 'Accounts: Guest account status' is set to 'Disabled' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy setting determines whether the Guest account is enabled or disabled. The Guest account allows unauthenticated network users to gain access to the system.

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

Note: This setting will have no impact when applied to the Domain Controllers organizational unit via group policy because Domain Controllers have no local account database. It can be configured at the domain level via group policy, similar to account lockout and password policy settings.

Rationale:

The default Guest account allows unauthenticated network users to log on as Guest with no password. These unauthorized users could access any resources that are accessible to the Guest account over the network. This capability means that any network shares with permissions that allow access to the Guest account, the Guests group, or the Everyone group will be accessible over the network, which could lead to the exposure or corruption of data.

Impact:

All network users will need to authenticate before they can access shared resources. If you disable the Guest account and the Network Access: Sharing and Security Model option is set to Guest Only, network logons, such as those performed by the Microsoft Network Server (SMB Service), will fail. This policy setting should have little impact on most organizations because it is the default setting in Microsoft Windows 2000, Windows XP, and Windows Server™ 2003.

Audit:

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

Remediation:

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

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

Default Value:

Disabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.7 Manage Default Accounts on Enterprise Assets and Software</u> Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.			
v7	<u>16.8 Disable Any Unassociated Accounts</u> Disable any account that cannot be associated with a business process or business owner.			

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

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting determines whether the Guest account is enabled or disabled. The Guest account allows unauthenticated network users to gain access to the system.

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

Note: The CIS recommended state for this setting is: **Disabled** on Member Servers **only**, which differs from the STIG recommended state of Members Servers and Domain Controllers.

Note #2: This setting will have no impact when applied to the Domain Controllers organizational unit via group policy because Domain Controllers have no local account database. It can be configured at the domain level via group policy, similar to account lockout and password policy settings.

Rationale:

The default Guest account allows unauthenticated network users to log on as Guest with no password. These unauthorized users could access any resources that are accessible to the Guest account over the network. This capability means that any network shares with permissions that allow access to the Guest account, the Guests group, or the Everyone group will be accessible over the network, which could lead to the exposure or corruption of data.

Impact:

All network users will need to authenticate before they can access shared resources. If you disable the Guest account and the Network Access: Sharing and Security Model option is set to Guest Only, network logons, such as those performed by the Microsoft Network Server (SMB Service), will fail. This policy setting should have little impact on most organizations because it is the default setting in Microsoft Windows 2000, Windows XP, and Windows Server™ 2003.

Audit:

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

Remediation:

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

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Guest account status

Default Value:

Disabled.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225024
Rule ID: SV-225024r569186_rule
STIG ID: WN16-SO-000010
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.7 Manage Default Accounts on Enterprise Assets and Software</u> Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.			
v7	<u>16.8 Disable Any Unassociated Accounts</u> Disable any account that cannot be associated with a business process or business owner.			

2.3.1.4 Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting determines whether local accounts that are not password protected can be used to log on from locations other than the physical computer console. If you enable this policy setting, local accounts that have blank passwords will not be able to log on to the network from remote client computers. Such accounts will only be able to log on at the keyboard of the computer.

The recommended state for this setting is: **Enabled**.

Rationale:

Blank passwords are a serious threat to computer security and should be forbidden through both organizational policy and suitable technical measures. In fact, the default settings for Active Directory domains require complex passwords of at least seven characters. However, if users with the ability to create new accounts bypass your domain-based password policies, they could create accounts with blank passwords. For example, a user could build a stand-alone computer, create one or more accounts with blank passwords, and then join the computer to the domain. The local accounts with blank passwords would still function. Anyone who knows the name of one of these unprotected accounts could then use it to log on.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SYSTEM\CurrentControlSet\Control\Lsa:LimitBlankPasswordUse
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Limit local account use of blank passwords to console logon only
```

Default Value:

Enabled.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225025
Rule ID: SV-225025r569186_rule
STIG ID: WN16-SO-000020
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			

2.3.1.5 Configure 'Accounts: Rename administrator account' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

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). On Domain Controllers, since they do not have their own local accounts, this rule refers to the built-in Administrator account that was established when the domain was first created.

Rationale:

The Administrator account exists on all computers that run the Windows 2000 or newer operating systems. If you rename this account, it is slightly more difficult for unauthorized persons to guess this privileged user name and password combination.

The built-in Administrator account cannot be locked out, regardless of how many times an attacker might use a bad password. This capability makes the Administrator account a popular target for brute force attacks that attempt to guess passwords. The value of this countermeasure is lessened because this account has a well-known SID, and there are third-party tools that allow authentication by using the SID rather than the account name. Therefore, even if you rename the Administrator account, an attacker could launch a brute force attack by using the SID to log on.

Impact:

You will have to inform users who are authorized to use this account of the new account name. (The guidance for this setting assumes that the Administrator account was not disabled, which was recommended earlier in this chapter.)

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, configure the following UI path:

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Rename administrator account

Default Value:

Administrator.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225026
Rule ID: SV-225026r569186_rule
STIG ID: WN16-SO-000030
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.7 Manage Default Accounts on Enterprise Assets and Software</u> Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.			

2.3.1.6 Configure 'Accounts: Rename guest account' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

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. On Domain Controllers, since they do not have their own local accounts, this rule refers to the built-in Guest account that was established when the domain was first created.

Rationale:

The Guest account exists on all computers that run the Windows 2000 or newer operating systems. If you rename this account, it is slightly more difficult for unauthorized persons to guess this privileged user name and password combination.

Impact:

There should be little impact, because the Guest account is disabled by default.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, configure the following UI path:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Rename guest account
```

Default Value:

Guest.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

```
Vul ID:      V-225027
Rule ID:     SV-225027r569186_rule
STIG ID:     WN16-SO-000040
Severity:    CAT II
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.7 Manage Default Accounts on Enterprise Assets and Software</u> Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.			

2.3.2 Audit

This section contains recommendations related to auditing controls.

2.3.2.1 Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting allows administrators to enable the more precise auditing capabilities present in Windows Vista.

The Audit Policy settings available in Windows Server 2003 Active Directory do not yet contain settings for managing the new auditing subcategories. To properly apply the auditing policies prescribed in this baseline, the Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings setting needs to be configured to Enabled.

The recommended state for this setting is: **Enabled**.

Important: Be very cautious about audit settings that can generate a large volume of traffic. For example, if you enable either success or failure auditing for all of the Privilege Use subcategories, the high volume of audit events generated can make it difficult to find other types of entries in the Security log. Such a configuration could also have a significant impact on system performance.

Rationale:

Prior to the introduction of auditing subcategories in Windows Vista, it was difficult to track events at a per-system or per-user level. The larger event categories created too many events and the key information that needed to be audited was difficult to find.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SYSTEM\CurrentControlSet\Control\Lsa:SCENoApplyLegacyAuditPolicy
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings
```

Default Value:

Enabled. (Advanced Audit Policy Configuration settings will be used for auditing configuration, and legacy Audit Policy configuration settings will be ignored.)

References:

1. <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing#to-ensure-that-advanced-audit-policy-configuration-settings-are-not-overwritten>

Additional Information:

```
Microsoft Windows Server 2016 Security Technical Implementation Guide:  
Version 2, Release 8, Benchmark Date: May 15, 2024
```

```
Vul ID: V-225028  
Rule ID: SV-225028r569186_rule  
STIG ID: WN16-SO-000050  
Severity: CAT II
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

2.3.2.2 Ensure 'Audit: Shut down system immediately if unable to log security audits' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether the system shuts down if it is unable to log Security events. It is a requirement for Trusted Computer System Evaluation Criteria (TCSEC)-C2 and Common Criteria certification to prevent auditable events from occurring if the audit system is unable to log them. Microsoft has chosen to meet this requirement by halting the system and displaying a stop message if the auditing system experiences a failure. When this policy setting is enabled, the system will be shut down if a security audit cannot be logged for any reason.

If the Audit: Shut down system immediately if unable to log security audits setting is enabled, unplanned system failures can occur. The administrative burden can be significant, especially if you also configure the Retention method for the Security log to Do not overwrite events (clear log manually). This configuration causes a repudiation threat (a backup operator could deny that they backed up or restored data) to become a denial of service (DoS) vulnerability, because a server could be forced to shut down if it is overwhelmed with logon events and other security events that are written to the Security log. Also, because the shutdown is not graceful, it is possible that irreparable damage to the operating system, applications, or data could result. Although the NTFS file system guarantees its integrity when an ungraceful computer shutdown occurs, it cannot guarantee that every data file for every application will still be in a usable form when the computer restarts.

The recommended state for this setting is: **Disabled**.

Rationale:

If the computer is unable to record events to the Security log, critical evidence or important troubleshooting information may not be available for review after a security incident. Also, an attacker could potentially generate a large volume of Security log events to purposely force a computer shutdown.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SYSTEM\CurrentControlSet\Control\Lsa:CrashOnAuditFail
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Audit: Shut down system immediately if unable to log security audits
```

Default Value:

Disabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 <u>Ensure Adequate Audit Log Storage</u> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.			
v7	6.4 <u>Ensure adequate storage for logs</u> Ensure that all systems that store logs have adequate storage space for the logs generated.			

2.3.3 DCOM

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

2.3.4 Devices

This section contains recommendations related to managing devices.

2.3.4.1 Ensure 'Devices: Prevent users from installing printer drivers' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

For a computer to print to a shared printer, the driver for that shared printer must be installed on the local computer. This security setting determines who is allowed to install a printer driver as part of connecting to a shared printer.

The recommended state for this setting is: **Enabled**.

Note: This setting does not affect the ability to add a local printer. This setting does not affect Administrators.

Rationale:

It may be appropriate in some organizations to allow users to install printer drivers on their own workstations. However, you should allow only Administrators, not users, to do so on servers, because printer driver installation on a server may unintentionally cause the computer to become less stable. A malicious user could install inappropriate printer drivers in a deliberate attempt to damage the computer, or a user might accidentally install malicious software that masquerades as a printer driver. It is feasible for an attacker to disguise a Trojan horse program as a printer driver. The program may appear to users as if they must use it to print, but such a program could unleash malicious code on your computer network.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SYSTEM\CurrentControlSet\Control\Print\Providers\LanMan Print  
Services\Servers:AddPrinterDrivers
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Devices: Prevent users from installing printer drivers
```

Default Value:

Enabled. (Only Administrators will be able to install a printer driver as part of connecting to a shared printer. The ability to add a local printer will not be affected.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			

2.3.5 Domain controller

This section contains recommendations related to Domain Controllers.

2.3.5.1 Ensure 'Domain controller: Allow server operators to schedule tasks' is set to 'Disabled' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This policy setting determines whether members of the Server Operators group are allowed to submit jobs by means of the AT schedule facility. The impact of this policy setting configuration should be small for most organizations. Users, including those in the Server Operators group, will still be able to create jobs by means of the Task Scheduler Wizard, but those jobs will run in the context of the account with which the user authenticates when they set up the job.

Note: An AT Service Account can be modified to select a different account rather than the LOCAL SYSTEM account. To change the account, open System Tools, click Scheduled Tasks, and then click Accessories folder. Then click AT Service Account on the Advanced menu.

The recommended state for this setting is: **Disabled**.

Rationale:

If you enable this policy setting, jobs that are created by server operators by means of the AT service will execute in the context of the account that runs that service. By default, that is the local SYSTEM account. If you enable this policy setting, server operators could perform tasks that SYSTEM is able to do but that they would typically not be able to do, such as add their account to the local Administrators group.

Impact:

None - this is the default behavior. Note that users (including those in the Server Operators group) are still able to create jobs by means of the Task Scheduler Wizard. However, those jobs will run in the context of the account that the user authenticates with when setting up the job.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

HKLM\SYSTEM\CurrentControlSet\Control\Lsa:SubmitControl

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain controller: Allow server operators to schedule tasks

Default Value:

Disabled. (Server Operators are not allowed to submit jobs by means of the AT schedule facility.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.5.2 Ensure 'Domain controller: Allow vulnerable Netlogon secure channel connections' is set to 'Not Configured' (DC Only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This security setting determines whether the domain controller bypasses secure RPC for Netlogon secure channel connections for specified machine accounts.

When deployed, this policy should be applied to all domain controllers in a forest by enabling the policy on the domain controllers OU.

When the **Create Vulnerable Connections** list (allow list) is configured:

- Given allow permission, the domain controller will allow accounts to use a Netlogon secure channel without secure RPC.
- Given deny permission, the domain controller will require accounts to use a Netlogon secure channel with secure RPC which is the same as the default (not necessary).

Note: Warning from Microsoft - enabling this policy will expose your domain-joined devices and can expose your Active Directory forest to risk. This policy should be used as a temporary measure for 3rd-party devices as you deploy updates. Once a 3rd-party device is updated to support using secure RPC with Netlogon secure channels, the account should be removed from the Create Vulnerable Connections list. To better understand the risk of configuring accounts to be allowed to use vulnerable Netlogon secure channel connections, please visit [How to manage the changes in Netlogon secure channel connections associated with CVE-2020-1472](#).

The recommended state for this setting is: **Not Configured**.

Rationale:

Enabling this policy will expose your domain-joined devices and can expose your Active Directory forest to security risks. It is highly recommended that this setting not be used (i.e. be left completely unconfigured) so as not to add risk.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location and when set properly a REG_SZ value of **does not exist**.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters\VulnerableChannelAllowList
```

Note: If this policy is set as prescribed, the registry key **vulnerablechannelallowlist**, will not be present in the above registry location.

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Not Configured**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain controller: Allow vulnerable Netlogon secure channel connections
```

Default Value:

Not Configured. (No machines or trust accounts are explicitly exempt from secure RPC with Netlogon secure channel connections enforcement.)

References:

1. <https://go.microsoft.com/fwlink/?linkid=2133485>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.5.3 Ensure 'Domain controller: LDAP server channel binding token requirements' is set to 'Always' (DC Only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This setting determines whether the LDAP server (Domain Controller) enforces validation of Channel Binding Tokens (CBT) received in LDAP bind requests that are sent over SSL/TLS (i.e. LDAPS).

The recommended state for this setting is: **Always**.

Note: All LDAP clients must have the [CVC-2017-8563](#) security update to be compatible with Domain Controllers that have this setting enabled. More information on this setting is available at: [MSKB 4520412: 2020 LDAP channel binding and LDAP signing requirements for Windows](#)

Rationale:

Requiring Channel Binding Tokens (CBT) can prevent an attacker who is able to capture users' authentication credentials (e.g. OAuth tokens, session identifiers, etc.) from reusing those credentials in another TLS session. This also helps to increase protection against "man-in-the-middle" attacks using LDAP authentication over SSL/TLS (LDAPS).

Impact:

All LDAP clients must provide channel binding information over SSL/TLS (i.e. LDAPS). The LDAP server (Domain Controller) rejects authentication requests from clients that do not do so. Clients must have the [CVC-2017-8563](#) security update to support this feature, and may have compatibility issues with this setting without the security update. This may also mean that LDAP authentication requests over SSL/TLS that previously worked may stop working until the security update is installed.

When first deploying this setting, you may **initially** want to only set it to the alternate setting of **When supported** (instead of **Always**) on all Domain Controllers. This alternate, **interim** setting enables support for LDAP client channel binding but does not *require* it. Then set one DC that is not currently being targeted by LDAP clients to **Always**, and test each of the critical LDAP clients against that DC (and remediating as necessary), before deploying **Always** to the rest of the DCs.

We also recommend using the new Event ID 3039 on your Domain Controllers (added with the March 2020 security update) to help locate clients that do not use Channel Binding Tokens (CBT) in their LDAPS connections. This new Event ID requires increasing the logging level of the **16 LDAP Interface Events** portion of the NTDS service diagnostics to a value of **2** (Basic). For more information, please see *Table 2: CBT events* at this link: [MSKB 4520412: 2020 LDAP channel binding and LDAP signing requirements for Windows](#)

Older OSES such as Windows XP, Windows Server 2003, Windows Vista and Windows Server 2008 (non-R2), will first require patches for [Microsoft Security Advisory 973811](#), as well as all associated fixes, in order to be compatible with domain controllers that have this setting deployed.

Note: Only **Always** is actually considered compliant to the CIS benchmark.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **2**.

```
HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters:LdapEnforceChannelBinding
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Always**:

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain controller: LDAP server channel binding token requirements

Note: This Group Policy path requires the installation of the March 2020 (or later) Windows security update. With that update, Microsoft added this setting to the built-in OS security template.

Default Value:

Never. (No LDAP channel binding validation is performed.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	16.5 <u>Encrypt Transmittal of Username and Authentication Credentials</u> Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.			

2.3.5.4 Ensure 'Domain controller: LDAP server signing requirements' is set to 'Require signing' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- STIG Domain Controller

Description:

This policy setting determines whether the Lightweight Directory Access Protocol (LDAP) server requires LDAP clients to negotiate data signing.

The recommended state for this setting is: **Require signing**.

Note: Domain member computers must have *Network security: LDAP signing requirements* (Rule 2.3.11.8) set to **Negotiate signing** or higher. If not, they will fail to authenticate once the above **Require signing** value is configured on the Domain Controllers. Fortunately, **Negotiate signing** is the default in the client configuration.

Note #2: This policy setting does not have any impact on LDAP simple bind (**ldap_simple_bind**) or LDAP simple bind through SSL (**ldap_simple_bind_s**). No Microsoft LDAP clients that are shipped with Windows XP Professional use LDAP simple bind or LDAP simple bind through SSL to talk to a Domain Controller.

Note #3: Before enabling this setting, you should first ensure that there are no clients (including server-based applications) that are configured to authenticate with Active Directory via unsigned LDAP, because changing this setting will break those applications. Such applications should first be reconfigured to use signed [LDAP, Secure LDAP \(LDAPS\), or IPsec-protected connections](#).

Rationale:

Unsigned network traffic is susceptible to man-in-the-middle attacks. In such attacks, an intruder captures packets between the server and the client, modifies them, and then forwards them to the client. Where LDAP servers are concerned, an attacker could cause a client to make decisions that are based on false records from the LDAP directory. To lower the risk of such an intrusion in an organization's network, you can implement strong physical security measures to protect the network infrastructure. Also, you could implement Internet Protocol security (IPsec) authentication header mode (AH), which performs mutual authentication and packet integrity for IP traffic to make all types of man-in-the-middle attacks extremely difficult.

Additionally, allowing the use of regular, unsigned LDAP permits credentials to be received over the network in clear text, which could very easily result in the interception of account passwords by other systems on the network.

Impact:

Unless TLS/SSL is being used, the LDAP data signing option must be negotiated. Clients that do not support LDAP signing will be unable to run LDAP queries against the Domain Controllers. All Windows 2000-based computers in your organization that are managed from Windows Server 2003-based or Windows XP-based computers and that use Windows NT Challenge/Response (NTLM) authentication must have Windows 2000 Service Pack 3 (SP3) installed. Alternatively, these clients must have a registry change. For information about this registry change, see Microsoft Knowledge Base article 325465: [Windows 2000 domain controllers require SP3 or later when using Windows Server 2003 administration tools](#). Also, some non-Microsoft operating systems do not support LDAP signing. If you enable this policy setting, client computers that use those operating systems may be unable to access domain resources.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **2**.

```
HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters:LDAPServerIntegrity
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Require signing**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain controller: LDAP server signing requirements
```

Default Value:

None. (Data signing is not required in order to bind with the server. If the client requests data signing, the server supports it.)

References:

1. <https://msrc.microsoft.com/update-guide/en-us/advisory/ADV190023>
2. <https://support.microsoft.com/en-us/topic/frequently-asked-questions-about-changes-to-lightweight-directory-access-protocol-41a40287-810a-e799-d067-f578fca055fc>

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224995
Rule ID: SV-224995r916422_rule
STIG ID: WN16-DC-000320
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			

2.3.5.5 Ensure 'Domain controller: Refuse machine account password changes' is set to 'Disabled' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- STIG Domain Controller

Description:

This security setting determines whether Domain Controllers will refuse requests from member computers to change computer account passwords.

The recommended state for this setting is: **Disabled**.

Note: Some problems can occur as a result of machine account password expiration, particularly if a machine is reverted to a previous point-in-time state, as is common with virtual machines. Depending on how far back the reversion is, the older machine account password stored on the machine may no longer be recognized by the domain controllers, and therefore the computer loses its domain trust. This can also disrupt non-persistent VDI implementations, and devices with write filters that disallow permanent changes to the OS volume. Some organizations may choose to exempt themselves from this recommendation and disable machine account password expiration for these situations.

Rationale:

If you enable this policy setting on all Domain Controllers in a domain, domain members will not be able to change their computer account passwords, and those passwords will be more susceptible to attack.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters:RefusePasswordChange
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain controller: Refuse machine account password changes
```

Default Value:

Disabled. (By default, member computers change their computer account passwords as specified by the *Domain member: Maximum machine account password age* setting (Rule 2.3.6.5), which is by default every 30 days.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224996
Rule ID: SV-224996r569186_rule
STIG ID: WN16-DC-000330
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

2.3.6 Domain member

This section contains recommendations related to domain membership.

2.3.6.1 Ensure 'Domain member: Digitally encrypt or sign secure channel data (always)' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting determines whether all secure channel traffic that is initiated by the domain member must be signed or encrypted.

The recommended state for this setting is: **Enabled**.

Rationale:

When a computer joins a domain, a computer account is created. After it joins the domain, the computer uses the password for that account to create a secure channel with the Domain Controller for its domain every time that it restarts. Requests that are sent on the secure channel are authenticated—and sensitive information such as passwords are encrypted—but the channel is not integrity-checked, and not all information is encrypted.

Digital encryption and signing of the secure channel is a good idea where it is supported. The secure channel protects domain credentials as they are sent to the Domain Controller.

Impact:

None - this is the default behavior. However, only Windows NT 4.0 with Service Pack 6a (SP6a) and subsequent versions of the Windows operating system support digital encryption and signing of the secure channel. Windows 98 Second Edition clients do not support it unless they have **Dsclient** installed. Therefore, you cannot enable the Domain member: Digitally encrypt or sign secure channel data (always) setting on Domain Controllers that support Windows 98 clients as members of the domain. Potential impacts can include the following:

- The ability to create or delete trust relationships with clients running versions of Windows earlier than Windows NT 4.0 with SP6a will be disabled.
- Logons from clients running versions of Windows earlier than Windows NT 4.0 with SP6a will be disabled.
- The ability to authenticate other domains' users from a Domain Controller running a version of Windows earlier than Windows NT 4.0 with SP6a in a trusted domain will be disabled.

You can enable this policy setting after you eliminate all Windows 9x clients from the domain and upgrade all Windows NT 4.0 servers and Domain Controllers from trusted/trusting domains to Windows NT 4.0 with SP6a.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters:RequireSignOrSeal
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Digitally encrypt or sign secure channel data (always)
```

Default Value:

Enabled. (All secure channel data must be signed or encrypted.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225029
Rule ID: SV-225029r916422_rule
STIG ID: WN16-SO-000080
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.			

2.3.6.2 Ensure 'Domain member: Digitally encrypt secure channel data (when possible)' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting determines whether a domain member should attempt to negotiate encryption for all secure channel traffic that it initiates.

The recommended state for this setting is: **Enabled**.

Rationale:

When a computer joins a domain, a computer account is created. After it joins the domain, the computer uses the password for that account to create a secure channel with the Domain Controller for its domain every time that it restarts. Requests that are sent on the secure channel are authenticated—and sensitive information such as passwords are encrypted—but the channel is not integrity-checked, and not all information is encrypted.

Digital encryption and signing of the secure channel is a good idea where it is supported. The secure channel protects domain credentials as they are sent to the Domain Controller.

Impact:

None - this is the default behavior. However, only Windows NT 4.0 Service Pack 6a (SP6a) and subsequent versions of the Windows operating system support digital encryption and signing of the secure channel. Windows 98 Second Edition clients do not support it unless they have **Dsclient** installed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters:SealSecureChannel
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Digitally encrypt secure channel data (when possible)
```

Default Value:

Enabled. (The domain member will request encryption of all secure channel traffic.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225030
Rule ID: SV-225030r916422_rule
STIG ID: WN16-SO-000090
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.			

2.3.6.3 Ensure 'Domain member: Digitally sign secure channel data (when possible)' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting determines whether a domain member should attempt to negotiate whether all secure channel traffic that it initiates must be digitally signed. Digital signatures protect the traffic from being modified by anyone who captures the data as it traverses the network.

The recommended state for this setting is: **Enabled**.

Rationale:

When a computer joins a domain, a computer account is created. After it joins the domain, the computer uses the password for that account to create a secure channel with the Domain Controller for its domain every time that it restarts. Requests that are sent on the secure channel are authenticated—and sensitive information such as passwords are encrypted—but the channel is not integrity-checked, and not all information is encrypted.

Digital encryption and signing of the secure channel is a good idea where it is supported. The secure channel protects domain credentials as they are sent to the Domain Controller.

Impact:

None - this is the default behavior. However, only Windows NT 4.0 with Service Pack 6a (SP6a) and subsequent versions of the Windows operating system support digital encryption and signing of the secure channel. Windows 98 Second Edition clients do not support it unless they have **Dsclient** installed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

HKLM\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters:SignSecureChannel

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Digitally sign secure channel data (when possible)

Default Value:

Enabled. (The domain member will request digital signing of all secure channel traffic.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225031
Rule ID: SV-225031r916422_rule
STIG ID: WN16-SO-000100
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			

2.3.6.4 Ensure 'Domain member: Disable machine account password changes' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting determines whether a domain member can periodically change its computer account password. Computers that cannot automatically change their account passwords are potentially vulnerable, because an attacker might be able to determine the password for the system's domain account.

The recommended state for this setting is: **Disabled**.

Note: Some problems can occur as a result of machine account password expiration, particularly if a machine is reverted to a previous point-in-time state, as is common with virtual machines. Depending on how far back the reversion is, the older machine account password stored on the machine may no longer be recognized by the domain controllers, and therefore the computer loses its domain trust. This can also disrupt non-persistent VDI implementations, and devices with write filters that disallow permanent changes to the OS volume. Some organizations may choose to exempt themselves from this recommendation and disable machine account password expiration for these situations.

Rationale:

The default configuration for Windows Server 2003-based computers that belong to a domain is that they are automatically required to change the passwords for their accounts every 30 days. If you disable this policy setting, computers that run Windows Server 2003 will retain the same passwords as their computer accounts. Computers that are no longer able to automatically change their account password are at risk from an attacker who could determine the password for the computer's domain account.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters:DisablePasswordChange
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Disable machine account password changes
```

Default Value:

Disabled. (The domain member can change its computer account password as specified by the recommendation *Domain Member: Maximum machine account password age*, which by default is every 30 days.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225032
Rule ID: SV-225032r877039_rule
STIG ID: WN16-SO-000110
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.6 <u>Centralize Account Management</u> Centralize account management through a directory or identity service.		●	●

2.3.6.5 Ensure 'Domain member: Maximum machine account password age' is set to '30 or fewer days, but not 0' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting determines the maximum allowable age for a computer account password. By default, domain members automatically change their domain passwords every 30 days.

The recommended state for this setting is: **30 or fewer days, but not 0.**

Note: A value of **0** does not conform to the benchmark as it disables maximum password age.

Note #2: Some problems can occur as a result of machine account password expiration, particularly if a machine is reverted to a previous point-in-time state, as is common with virtual machines. Depending on how far back the reversion is, the older machine account password stored on the machine may no longer be recognized by the domain controllers, and therefore the computer loses its domain trust. This can also disrupt non-persistent VDI implementations, and devices with write filters that disallow permanent changes to the OS volume. Some organizations may choose to exempt themselves from this recommendation and disable machine account password expiration for these situations.

Rationale:

In Active Directory-based domains, each computer has an account and password just like every user. By default, the domain members automatically change their domain password every 30 days. If you increase this interval significantly, or set it to 0 so that the computers no longer change their passwords, an attacker will have more time to undertake a brute force attack to guess the passwords of computer accounts.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a REG_DWORD value of **30** or less, but not **0**

HKLM\System\CurrentControlSet\Services\Netlogon\Parameters:MaximumPasswordAge

Remediation:

To establish the recommended configuration via GP, set the following UI path to **30 or fewer days, but not 0**:

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Maximum machine account password age

Default Value:

30 days.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225033
Rule ID: SV-225033r569186_rule
STIG ID: WN16-SO-000120
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			

2.3.6.6 Ensure 'Domain member: Require strong (Windows 2000 or later) session key' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

When this policy setting is enabled, a secure channel can only be established with Domain Controllers that are capable of encrypting secure channel data with a strong (128-bit) session key.

To enable this policy setting, all Domain Controllers in the domain must be able to encrypt secure channel data with a strong key, which means all Domain Controllers must be running Microsoft Windows 2000 or newer.

The recommended state for this setting is: **Enabled**.

Rationale:

Session keys that are used to establish secure channel communications between Domain Controllers and member computers are much stronger in Windows 2000 than they were in previous Microsoft operating systems. Whenever possible, you should take advantage of these stronger session keys to help protect secure channel communications from attacks that attempt to hijack network sessions and eavesdropping. (Eavesdropping is a form of hacking in which network data is read or altered in transit. The data can be modified to hide or change the sender, or be redirected.)

Impact:

None - this is the default behavior. However, computers will not be able to join Windows NT 4.0 domains, and trusts between Active Directory domains and Windows NT-style domains may not work properly. Also, Domain Controllers with this setting configured will not allow older pre-Windows 2000 clients (that do not support this policy setting) to join the domain.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters:RequireStrongKey
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Require strong (Windows 2000 or later) session key
```

Default Value:

Enabled. (The secure channel will not be established unless 128-bit encryption can be performed.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225034
Rule ID: SV-225034r916422_rule
STIG ID: WN16-SO-000130
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			

2.3.7 Interactive logon

This section contains recommendations related to interactive logons.

2.3.7.1 Ensure 'Interactive logon: Do not display last user name' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether the account name of the last user to log on to the client computers in your organization will be displayed in each computer's respective Windows logon screen. Enable this policy setting to prevent intruders from collecting account names visually from the screens of desktop or laptop computers in your organization.

The recommended state for this setting is: **Enabled**.

Rationale:

An attacker with access to the console (for example, someone with physical access or someone who is able to connect to the server through Remote Desktop Services) could view the name of the last user who logged on to the server. The attacker could then try to guess the password, use a dictionary, or use a brute-force attack to try and log on.

Impact:

The name of the last user to successfully log on will not be displayed in the Windows logon screen.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:DontDisplayLastUserName
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Do not display last user name
```

Note: In newer versions of Microsoft Windows Server, starting with Windows Server 2019, this setting was renamed *Interactive logon: Don't display last signed-in*.

Default Value:

Disabled. (The name of the last user to log on is displayed in the Windows logon screen.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.7.2 Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether users must press CTRL+ALT+DEL before they log on.

The recommended state for this setting is: **Disabled**.

Rationale:

Microsoft developed this feature to make it easier for users with certain types of physical impairments to log on to computers that run Windows. If users are not required to press CTRL+ALT+DEL, they are susceptible to attacks that attempt to intercept their passwords. If CTRL+ALT+DEL is required before logon, user passwords are communicated by means of a trusted path.

An attacker could install a Trojan horse program that looks like the standard Windows logon dialog box and capture the user's password. The attacker would then be able to log on to the compromised account with whatever level of privilege that user has.

Impact:

Users must press CTRL+ALT+DEL before they log on to Windows unless they use a smart card for Windows logon. A smart card is a tamper-proof device that stores security information.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:DisableCAD
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Do not require CTRL+ALT+DEL

Default Value:

On Windows Server 2008 R2 or older: Disabled.

On Windows Server 2012 (non-R2) or newer: Enabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.10 Enforce Automatic Device Lockout on Portable End-User Devices</u> Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts.			

2.3.7.3 Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

Windows notices inactivity of a logon session, and if the amount of inactive time exceeds the inactivity limit, then the screen saver will run, locking the session.

The recommended state for this setting is: **900 or fewer second(s), but not 0.**

Note: A value of **0** does not conform to the benchmark as it disables the machine inactivity limit.

Rationale:

If a user forgets to lock their computer when they walk away it's possible that a passerby will hijack it.

Impact:

The screen saver will automatically activate when the computer has been unattended for the amount of time specified. The impact should be minimal since the screen saver is enabled by default.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a REG_DWORD value of **900** or less, but not **0**

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:  
InactivityTimeoutSecs
```


Remediation:

To establish the recommended configuration via GP, set the following UI path to **900 or fewer seconds, but not 0**:

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Machine inactivity limit

Default Value:

0 seconds. (There is no inactivity limit).

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225035
Rule ID: SV-225035r569186_rule
STIG ID: WN16-SO-000140
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u> Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.			
v7	16.11 <u>Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity.			

2.3.7.4 Configure 'Interactive logon: Message text for users attempting to log on' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting specifies a text message that displays to users when they log on. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale:

Displaying a warning message before logon may help prevent an attack by warning the attacker about the consequences of their misconduct before it happens. It may also help to reinforce corporate policy by notifying employees of the appropriate policy during the logon process. This text is often used for legal reasons—for example, to warn users about the ramifications of misusing company information or to warn them that their actions may be audited.

Note: Any warning that you display should first be approved by your organization's legal and human resources representatives.

Impact:

Users will have to acknowledge a dialog box containing the configured text before they can log on to the computer.

Note: Windows Vista and Windows XP Professional support logon banners that can exceed 512 characters in length and that can also contain carriage-return line-feed sequences. However, Windows 2000-based clients cannot interpret and display these messages. You must use a Windows 2000-based computer to create a logon message policy that applies to Windows 2000-based computers.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_SZ** value of **text**.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:  
LegalNoticeText
```

Remediation:

To establish the recommended configuration via GP, configure the following UI path to a value that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local  
Policies\Security Options\Interactive logon: Message text for users  
attempting to log on
```

Default Value:

No message.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225036
Rule ID: SV-225036r569186_rule
STIG ID: WN16-SO-000150
Severity: CAT II

Message Text for STIG Compliance:

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.7.5 Configure 'Interactive logon: Message title for users attempting to log on' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting specifies the text displayed in the title bar of the window that users see when they log on to the system. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale:

Displaying a warning message before logon may help prevent an attack by warning the attacker about the consequences of their misconduct before it happens. It may also help to reinforce corporate policy by notifying employees of the appropriate policy during the logon process.

Impact:

Users will have to acknowledge a dialog box with the configured title before they can log on to the computer.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_SZ** value of **text**.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:  
LegalNoticeCaption
```

Remediation:

To establish the recommended configuration via GP, configure the following UI path to a value that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Message title for users attempting to log on
```

Default Value:

No message.

Additional Information:

```
Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID:    V-225037
Rule ID:   SV-225037r569186_rule
STIG ID:   WN16-SO-000160
Severity:  CAT II
```

Message Text for STIG Compliance:

- DoD Notice and Consent Banner
- US Department of Defense Warning Statement
- Or an organization-defined equivalent

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.7.6 Ensure 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' is set to '4 or fewer logon(s)' (MS only) (Automated)

Profile Applicability:

- Level 2 - Member Server
- STIG Member Server

Description:

This policy setting determines whether a user can log on to a Windows domain using cached account information. Logon information for domain accounts can be cached locally to allow users to log on even if a Domain Controller cannot be contacted. This policy setting determines the number of unique users for whom logon information is cached locally. If this value is set to 0, the logon cache feature is disabled. An attacker who is able to access the file system of the server could locate this cached information and use a brute force attack to determine user passwords.

The recommended state for this setting is: **4 or fewer logon(s)**.

Rationale:

The number that is assigned to this policy setting indicates the number of users whose logon information the computer will cache locally. If the number is set to 4, then the computer caches logon information for 4 users. When a 5th user logs on to the computer, the server overwrites the oldest cached logon session.

Users who access the computer console will have their logon credentials cached on that computer. An attacker who is able to access the file system of the computer could locate this cached information and use a brute force attack to attempt to determine user passwords. To mitigate this type of attack, Windows encrypts the information and obscures its physical location.

Impact:

Users will be unable to log on to any computers if there is no Domain Controller available to authenticate them. Organizations may want to configure this value to 2 for end-user computers, especially for mobile users. A configuration value of 2 means that the user's logon information will still be in the cache, even if a member of the IT department has recently logged on to their computer to perform system maintenance. This method allows users to log on to their computers when they are not connected to the organization's network.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\Winlogon:CachedLogonsCount
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **4 or fewer logon(s)**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local  
Policies\Security Options\Interactive logon: Number of previous logons to  
cache (in case domain controller is not available)
```

Default Value:

On Windows Server 2008 (non-R2): 25 logons.

On Windows Server 2008 R2 or newer: 10 logons.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225011
Rule ID: SV-225011r857264_rule
STIG ID: WN16-MS-000050
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.7.7 Ensure 'Interactive logon: Prompt user to change password before expiration' is set to 'between 5 and 14 days' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines how far in advance users are warned that their password will expire. It is recommended that you configure this policy setting to at least 5 days but no more than 14 days to sufficiently warn users when their passwords will expire.

The recommended state for this setting is: **between 5 and 14 days**.

Rationale:

It is recommended that user passwords be configured to expire periodically. Users will need to be warned that their passwords are going to expire, or they may inadvertently be locked out of the computer when their passwords expire. This condition could lead to confusion for users who access the network locally, or make it impossible for users to access your organization's network through dial-up or virtual private network (VPN) connections.

Impact:

Users will see a dialog box prompt to change their password each time that they log on to the domain when their password is configured to expire between 5 and 14 days.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value between **5** and **14**.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\Winlogon:PasswordExpiryWarning
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to a value **between 5 and 14 days**:

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Prompt user to change password before expiration

Default Value:

5 days.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.7.8 Ensure 'Interactive logon: Require Domain Controller Authentication to unlock workstation' is set to 'Enabled' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

Logon information is required to unlock a locked computer. For domain accounts, this security setting determines whether it is necessary to contact a Domain Controller to unlock a computer.

The recommended state for this setting is: **Enabled**.

Rationale:

By default, the computer caches in memory the credentials of any users who are authenticated locally. The computer uses these cached credentials to authenticate anyone who attempts to unlock the console. When cached credentials are used, any changes that have recently been made to the account — such as user rights assignments, account lockout, or the account being disabled — are not considered or applied after the account is authenticated. User privileges are not updated, and (more importantly) disabled accounts are still able to unlock the console of the computer.

Impact:

When the console on a computer is locked, either by a user or automatically by a screen saver time-out, the console can only be unlocked if a Domain Controller is available to re-authenticate the domain account that is being used to unlock the computer. If no Domain Controller is available, the user cannot unlock the computer.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon:ForceUnlockLogon

Remediation:

To implement the recommended configuration via GP, set the following UI path to **Enabled**:

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Require Domain Controller Authentication to unlock workstation

Default Value:

Disabled. (Logon information confirmation with a Domain Controller is not required for a user to unlock the computer, and the user can unlock the computer using cached credentials, if they are present.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u> Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.			
v7	16.11 <u>Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity.			

2.3.7.9 Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines what happens when the smart card for a logged-on user is removed from the smart card reader.

The recommended state for this setting is: **Lock Workstation**. Configuring this setting to **Force Logoff** or **Disconnect if a Remote Desktop Services session** also conforms to the benchmark.

Rationale:

Users sometimes forget to lock their workstations when they are away from them, allowing the possibility for malicious users to access their computers. If smart cards are used for authentication, the computer should automatically lock itself when the card is removed to ensure that only the user with the smart card is accessing resources using those credentials.

Impact:

If you select **Lock Workstation**, the workstation is locked when the smart card is removed, allowing users to leave the area, take their smart card with them, and still maintain a protected session.

If you select **Force Logoff**, users are automatically logged off when their smart card is removed.

If you select **Disconnect if a Remote Desktop Services session**, removal of the smart card disconnects the session without logging the users off. This allows the user to insert the smart card and resume the session later, or at another smart card reader-equipped computer, without having to log on again. If the session is local, this policy will function identically to **Lock Workstation**.

Enforcing this setting on computers used by people who must log onto multiple computers in order to perform their duties could be frustrating and lower productivity. For example, if network administrators are limited to a single account but need to log into several computers simultaneously in order to effectively manage the network enforcing this setting will limit them to logging onto one computer at a time. For these reasons it is recommended that this setting only be enforced on workstations used for purposes commonly associated with typical users such as document creation and email.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_SZ** value of **1**, **2**, or **3**.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\Winlogon:ScRemoveOption
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Lock Workstation** (or, if applicable for your environment, **Force Logoff** or **Disconnect if a Remote Desktop Services session**):

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local  
Policies\Security Options\Interactive logon: Smart card removal behavior
```

Default Value:

No action.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u> Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.			
v7	16.11 <u>Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity.			

2.3.7.10 Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or 'Force Logoff' (STIG only) (Automated)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting determines what happens when the smart card for a logged-on user is removed from the smart card reader.

The recommended STIG state for this setting is: **Lock Workstation** or **Force Logoff**.

Note: The CIS recommended state for this setting is: **Lock Workstation** or higher, which differs from the STIG recommended state. Configuring this setting to **Force Logoff** or **Disconnect if a Remote Desktop Services session** also conforms to the CIS recommended state.

Rationale:

Users sometimes forget to lock their workstations when they are away from them, allowing the possibility for malicious users to access their computers. If smart cards are used for authentication, the computer should automatically lock itself when the card is removed to ensure that only the user with the smart card is accessing resources using those credentials.

Impact:

If you select **Lock Workstation**, the workstation is locked when the smart card is removed, allowing users to leave the area, take their smart card with them, and still maintain a protected session.

If you select **Force Logoff**, users are automatically logged off when their smart card is removed.

If you select **Disconnect if a Remote Desktop Services session**, removal of the smart card disconnects the session without logging the users off. This allows the user to insert the smart card and resume the session later, or at another smart card reader-equipped computer, without having to log on again. If the session is local, this policy will function identically to **Lock Workstation**.

Enforcing this setting on computers used by people who must log onto multiple computers in order to perform their duties could be frustrating and lower productivity. For example, if network administrators are limited to a single account but need to log into several computers simultaneously in order to effectively manage the network enforcing this setting will limit them to logging onto one computer at a time. For these reasons it is recommended that this setting only be enforced on workstations used for purposes commonly associated with typical users such as document creation and email.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed, noting that values of **Force Logoff** or **Disconnect if a Remote Desktop Services session** are also acceptable settings. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\Winlogon:ScRemoveOption
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Lock Workstation** (or, if applicable for your environment, **Force Logoff** or **Disconnect if a Remote Desktop Services session**):

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local  
Policies\Security Options\Interactive logon: Smart card removal behavior
```

Default Value:

No action.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225038
Rule ID: SV-225038r569186_rule
STIG ID: WN16-SO-000180
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u> Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.			
v7	16.11 <u>Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity.			

2.3.8 Microsoft network client

This section contains recommendations related to configuring the Microsoft network client.

2.3.8.1 Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting determines whether packet signing is required by the SMB client component.

Note: When Windows Vista-based computers have this policy setting enabled and they connect to file or print shares on remote servers, it is important that the setting is synchronized with its companion setting, **Microsoft network server: Digitally sign communications (always)**, on those servers. For more information about these settings, see the "Microsoft network client and server: Digitally sign communications (four related settings)" section in Chapter 5 of the Threats and Countermeasures guide.

The recommended state for this setting is: **Enabled**.

Rationale:

Session hijacking uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers can potentially intercept and modify unsigned SMB packets and then modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after legitimate authentication and gain unauthorized access to data.

SMB is the resource sharing protocol that is supported by many Windows operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place.

Impact:

The Microsoft network client will not communicate with a Microsoft network server unless that server agrees to perform SMB packet signing.

The Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, Windows XP Professional and Windows Vista implementations of the SMB file and print sharing protocol support mutual authentication, which prevents session hijacking attacks and supports message authentication to prevent man-in-the-middle attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server.

Implementation of SMB signing may negatively affect performance, because each packet needs to be signed and verified. If these settings are enabled on a server that is performing multiple roles, such as a small business server that is serving as a Domain Controller, file server, print server, and application server performance may be substantially slowed. Additionally, if you configure computers to ignore all unsigned SMB communications, older applications and operating systems will not be able to connect. However, if you completely disable all SMB signing, computers will be vulnerable to session hijacking attacks.

When SMB signing policies are enabled on Domain Controllers running Windows Server 2003 and member computers running Windows Vista SP1 or Windows Server 2008 group policy processing will fail. A hotfix is available from Microsoft that resolves this issue; see Microsoft Knowledge Base article 950876 for more details: [Group Policy settings are not applied on member computers that are running Windows Server 2008 or Windows Vista SP1 when certain SMB signing policies are enabled](#).

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters:RequireSecuritySignature
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network client: Digitally sign communications (always)
```

Default Value:

Disabled. (SMB packet signing is negotiated between the client and server.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225039
Rule ID: SV-225039r916422_rule
STIG ID: WN16-SO-000190
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			

2.3.8.2 Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting determines whether the SMB client will attempt to negotiate SMB packet signing.

Note: Enabling this policy setting on SMB clients on your network makes them fully effective for packet signing with all clients and servers in your environment.

The recommended state for this setting is: **Enabled**.

Rationale:

Session hijacking uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers can potentially intercept and modify unsigned SMB packets and then modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after legitimate authentication and gain unauthorized access to data.

SMB is the resource sharing protocol that is supported by many Windows operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place.

Impact:

None - this is the default behavior.

The Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, Windows XP Professional and Windows Vista implementations of the SMB file and print sharing protocol support mutual authentication, which prevents session hijacking attacks and supports message authentication to prevent man-in-the-middle attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server.

Implementation of SMB signing may negatively affect performance, because each packet needs to be signed and verified. If these settings are enabled on a server that is performing multiple roles, such as a small business server that is serving as a Domain Controller, file server, print server, and application server performance may be substantially slowed. Additionally, if you configure computers to ignore all unsigned SMB communications, older applications and operating systems will not be able to connect. However, if you completely disable all SMB signing, computers will be vulnerable to session hijacking attacks.

When SMB signing policies are enabled on Domain Controllers running Windows Server 2003 and member computers running Windows Vista SP1 or Windows Server 2008 group policy processing will fail. A hotfix is available from Microsoft that resolves this issue; see Microsoft Knowledge Base article 950876 for more details: [Group Policy settings are not applied on member computers that are running Windows Server 2008 or Windows Vista SP1 when certain SMB signing policies are enabled](#).

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters:EnableSecuritySignature
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network client: Digitally sign communications (if server agrees)
```

Default Value:

Enabled. (The Microsoft network client will ask the server to perform SMB packet signing upon session setup. If packet signing has been enabled on the server, packet signing will be negotiated.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225040
Rule ID: SV-225040r916422_rule
STIG ID: WN16-SO-000200
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			

2.3.8.3 Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting determines whether the SMB redirector will send plaintext passwords during authentication to third-party SMB servers that do not support password encryption.

It is recommended that you disable this policy setting unless there is a strong business case to enable it. If this policy setting is enabled, unencrypted passwords will be allowed across the network.

The recommended state for this setting is: **Disabled**.

Rationale:

If you enable this policy setting, the server can transmit passwords in plaintext across the network to other computers that offer SMB services, which is a significant security risk. These other computers may not use any of the SMB security mechanisms that are included with Windows Server 2003.

Impact:

None - this is the default behavior.

Some very old applications and operating systems such as MS-DOS, Windows for Workgroups 3.11, and Windows 95a may not be able to communicate with the servers in your organization by means of the SMB protocol.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters:EnablePlainTextPassword
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network client: Send unencrypted password to third-party SMB servers
```

Default Value:

Disabled. (Plaintext passwords will not be sent during authentication to third-party SMB servers that do not support password encryption.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225041
Rule ID: SV-225041r877396_rule
STIG ID: WN16-SO-000210
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	16.4 <u>Encrypt or Hash all Authentication Credentials</u> Encrypt or hash with a salt all authentication credentials when stored.		●	●

2.3.9 Microsoft network server

This section contains recommendations related to configuring the Microsoft network server.

2.3.9.1 Ensure 'Microsoft network server: Amount of idle time required before suspending session' is set to '15 or fewer minute(s)' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to specify the amount of continuous idle time that must pass in an SMB session before the session is suspended because of inactivity. Administrators can use this policy setting to control when a computer suspends an inactive SMB session. If client activity resumes, the session is automatically reestablished.

The maximum value is 99999, which is over 69 days; in effect, this value disables the setting.

The recommended state for this setting is: **15 or fewer minute(s)**.

Rationale:

Each SMB session consumes server resources, and numerous null sessions will slow the server or possibly cause it to fail. An attacker could repeatedly establish SMB sessions until the server's SMB services become slow or unresponsive.

Impact:

There will be little impact because SMB sessions will be re-established automatically if the client resumes activity.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **15** or less.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters:  
AutoDisconnect
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **15 or fewer minute(s)**:

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Amount of idle time required before suspending session

Default Value:

15 minutes.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.9.2 Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting determines whether packet signing is required by the SMB server component. Enable this policy setting in a mixed environment to prevent downstream clients from using the workstation as a network server.

The recommended state for this setting is: **Enabled**.

Rationale:

Session hijacking uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers can potentially intercept and modify unsigned SMB packets and then modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after legitimate authentication and gain unauthorized access to data.

SMB is the resource sharing protocol that is supported by many Windows operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place.

Impact:

The Microsoft network server will not communicate with a Microsoft network client unless that client agrees to perform SMB packet signing.

The Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, Windows XP Professional and Windows Vista implementations of the SMB file and print sharing protocol support mutual authentication, which prevents session hijacking attacks and supports message authentication to prevent man-in-the-middle attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server.

Implementation of SMB signing may negatively affect performance, because each packet needs to be signed and verified. If these settings are enabled on a server that is performing multiple roles, such as a small business server that is serving as a Domain Controller, file server, print server, and application server performance may be substantially slowed. Additionally, if you configure computers to ignore all unsigned SMB communications, older applications and operating systems will not be able to connect. However, if you completely disable all SMB signing, computers will be vulnerable to session hijacking attacks.

When SMB signing policies are enabled on Domain Controllers running Windows Server 2003 and member computers running Windows Vista SP1 or Windows Server 2008 group policy processing will fail. A hotfix is available from Microsoft that resolves this issue; see Microsoft Knowledge Base article 950876 for more details: [Group Policy settings are not applied on member computers that are running Windows Server 2008 or Windows Vista SP1 when certain SMB signing policies are enabled](#).

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters:RequireSecuritySignature
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Digitally sign communications (always)
```

Default Value:

On Member Servers: Disabled. (SMB packet signing is negotiated between the client and server.)

On Domain Controllers: Enabled. (The Microsoft network server will not communicate with a Microsoft network client unless that client agrees to perform SMB packet signing.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225042
Rule ID: SV-225042r916422_rule
STIG ID: WN16-SO-000230
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			

2.3.9.3 Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting determines whether the SMB server will negotiate SMB packet signing with clients that request it. If no signing request comes from the client, a connection will be allowed without a signature if the **Microsoft network server: Digitally sign communications (always)** setting is not enabled.

Note: Enable this policy setting on SMB clients on your network to make them fully effective for packet signing with all clients and servers in your environment.

The recommended state for this setting is: **Enabled**.

Rationale:

Session hijacking uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers can potentially intercept and modify unsigned SMB packets and then modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after legitimate authentication and gain unauthorized access to data.

SMB is the resource sharing protocol that is supported by many Windows operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place.

Impact:

The Microsoft network server will negotiate SMB packet signing as requested by the client. That is, if packet signing has been enabled on the client, packet signing will be negotiated.

The Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, Windows XP Professional and Windows Vista implementations of the SMB file and print sharing protocol support mutual authentication, which prevents session hijacking attacks and supports message authentication to prevent man-in-the-middle attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server.

Implementation of SMB signing may negatively affect performance, because each packet needs to be signed and verified. If these settings are enabled on a server that is performing multiple roles, such as a small business server that is serving as a Domain Controller, file server, print server, and application server performance may be substantially slowed. Additionally, if you configure computers to ignore all unsigned SMB communications, older applications and operating systems will not be able to connect. However, if you completely disable all SMB signing, computers will be vulnerable to session hijacking attacks.

When SMB signing policies are enabled on Domain Controllers running Windows Server 2003 and member computers running Windows Vista SP1 or Windows Server 2008 group policy processing will fail. A hotfix is available from Microsoft that resolves this issue; see Microsoft Knowledge Base article 950876 for more details: [Group Policy settings are not applied on member computers that are running Windows Server 2008 or Windows Vista SP1 when certain SMB signing policies are enabled](#).

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters:EnableSecuritySignature
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Digitally sign communications (if client agrees)
```

Default Value:

On Member Servers: Disabled. (The SMB client will never negotiate SMB packet signing.)

On Domain Controllers: Enabled. (The Microsoft network server will negotiate SMB packet signing as requested by the client. That is, if packet signing has been enabled on the client, packet signing will be negotiated.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225043
Rule ID: SV-225043r916422_rule
STIG ID: WN16-SO-000240
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			

2.3.9.4 Ensure 'Microsoft network server: Disconnect clients when logon hours expire' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This security setting determines whether to disconnect users who are connected to the local computer outside their user account's valid logon hours. This setting affects the Server Message Block (SMB) component. If you enable this policy setting you should also enable *Network security: Force logoff when logon hours expire* (Rule 2.3.11.6).

If your organization configures logon hours for users, this policy setting is necessary to ensure they are effective.

The recommended state for this setting is: **Enabled**.

Rationale:

If your organization configures logon hours for users, then it makes sense to enable this policy setting. Otherwise, users who should not have access to network resources outside of their logon hours may actually be able to continue to use those resources with sessions that were established during allowed hours.

Impact:

None - this is the default behavior. If logon hours are not used in your organization, this policy setting will have no impact. If logon hours are used, existing user sessions will be forcibly terminated when their logon hours expire.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters:enableforcedlogoff
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Disconnect clients when logon hours expire

Default Value:

Enabled. (Client sessions with the SMB service are forcibly disconnected when the client's logon hours expire.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	16.13 <u>Alert on Account Login Behavior Deviation</u> Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

2.3.9.5 Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy setting controls the level of validation a computer with shared folders or printers (the server) performs on the service principal name (SPN) that is provided by the client computer when it establishes a session using the server message block (SMB) protocol.

The server message block (SMB) protocol provides the basis for file and print sharing and other networking operations, such as remote Windows administration. The SMB protocol supports validating the SMB server service principal name (SPN) within the authentication blob provided by a SMB client to prevent a class of attacks against SMB servers referred to as SMB relay attacks. This setting will affect both SMB1 and SMB2.

The recommended state for this setting is: **Accept if provided by client**. Configuring this setting to **Required from client** also conforms to the benchmark.

Note: Since the release of the MS [KB3161561](#) security patch, this setting can cause significant issues (such as replication problems, group policy editing issues and blue screen crashes) on Domain Controllers when used *simultaneously* with UNC path hardening (i.e. Rule 18.5.14.1). **CIS therefore recommends against deploying this setting on Domain Controllers.**

Rationale:

The identity of a computer can be spoofed to gain unauthorized access to network resources.

Impact:

All Windows operating systems support both a client-side SMB component and a server-side SMB component. This setting affects the server SMB behavior, and its implementation should be carefully evaluated and tested to prevent disruptions to file and print serving capabilities.

If configured to **Accept if provided by client**, the SMB server will accept and validate the SPN provided by the SMB client and allow a session to be established if it matches the SMB server's list of SPN's for itself. If the SPN does NOT match, the session request for that SMB client will be denied.

If configured to **Required from client**, the SMB client MUST send a SPN name in session setup, and the SPN name provided MUST match the SMB server that is being requested to establish a connection. If no SPN is provided by client, or the SPN provided does not match, the session is denied.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters:SMBServerNameHardeningLevel
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Accept if provided by client** (configuring to **Required from client** also conforms to the benchmark):

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Server SPN target name validation level
```

Default Value:

Off. (The SPN is not required or validated by the SMB server from a SMB client.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

2.3.10 Network access

This section contains recommendations related to network access.

2.3.10.1 Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting determines whether an anonymous user can request security identifier (SID) attributes for another user, or use a SID to obtain its corresponding user name.

The recommended state for this setting is: **Disabled**.

Rationale:

If this policy setting is enabled, a user with local access could use the well-known Administrator's SID to learn the real name of the built-in Administrator account, even if it has been renamed. That person could then use the account name to initiate a password guessing attack.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa:TurnOffAnonymousBlock
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Allow anonymous SID/Name translation
```

Default Value:

Disabled. (An anonymous user cannot request the SID attribute for another user.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225044
Rule ID: SV-225044r569186_rule
STIG ID: WN16-SO-000250
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.10.2 Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy setting controls the ability of anonymous users to enumerate the accounts in the Security Accounts Manager (SAM). If you enable this policy setting, users with anonymous connections will not be able to enumerate domain account user names on the systems in your environment. This policy setting also allows additional restrictions on anonymous connections.

The recommended state for this setting is: **Enabled**.

Note: This policy has no effect on Domain Controllers.

Rationale:

An unauthorized user could anonymously list account names and use the information to attempt to guess passwords or perform social engineering attacks. (Social engineering attacks try to deceive users in some way to obtain passwords or some form of security information.)

Impact:

None - this is the default behavior. It will be impossible to establish trusts with Windows NT 4.0-based domains. Also, client computers that run older versions of the Windows operating system such as Windows NT 3.51 and Windows 95 will experience problems when they try to use resources on the server.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

HKLM\SYSTEM\CurrentControlSet\Control\Lsa:RestrictAnonymousSAM

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow anonymous enumeration of SAM accounts

Default Value:

Enabled. (Do not allow anonymous enumeration of SAM accounts. This option replaces Everyone with Authenticated Users in the security permissions for resources.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.10.3 Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled' (STIG only) (Automated)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting controls the ability of anonymous users to enumerate the accounts in the Security Accounts Manager (SAM). If you enable this policy setting, users with anonymous connections will not be able to enumerate domain account user names on the systems in your environment. This policy setting also allows additional restrictions on anonymous connections.

The recommended STIG state for this setting is: **Enabled**.

The recommended CIS state for this setting is: **Enabled** on Member Servers only.

Note: This policy has no effect on Domain Controllers.

Rationale:

An unauthorized user could anonymously list account names and use the information to attempt to guess passwords or perform social engineering attacks. (Social engineering attacks try to deceive users in some way to obtain passwords or some form of security information.)

Impact:

None - this is the default behavior. It will be impossible to establish trusts with Windows NT 4.0-based domains. Also, client computers that run older versions of the Windows operating system such as Windows NT 3.51 and Windows 95 will experience problems when they try to use resources on the server.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa:RestrictAnonymousSAM

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local  
Policies\Security Options\Network access: Do not allow anonymous enumeration  
of SAM accounts
```

Default Value:

Enabled. (Do not allow anonymous enumeration of SAM accounts. This option replaces Everyone with Authenticated Users in the security permissions for resources.)

Additional Information:

```
Microsoft Windows Server 2016 Security Technical Implementation Guide:  
Version 2, Release 8, Benchmark Date: May 15, 2024
```

```
Vul ID:    V-225045  
Rule ID:   SV-225045r569186_rule  
STIG ID:   WN16-SO-000260  
Severity:  CAT II
```

2.3.10.4 Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy setting controls the ability of anonymous users to enumerate SAM accounts as well as shares. If you enable this policy setting, anonymous users will not be able to enumerate domain account user names and network share names on the systems in your environment.

The recommended state for this setting is: **Enabled**.

Note: This policy has no effect on Domain Controllers.

Rationale:

An unauthorized user could anonymously list account names and shared resources and use the information to attempt to guess passwords or perform social engineering attacks. (Social engineering attacks try to deceive users in some way to obtain passwords or some form of security information.)

Impact:

It will be impossible to establish trusts with Windows NT 4.0-based domains. Also, client computers that run older versions of the Windows operating system such as Windows NT 3.51 and Windows 95 will experience problems when they try to use resources on the server. Users who access file and print servers anonymously will be unable to list the shared network resources on those servers; the users will have to authenticate before they can view the lists of shared folders and printers. However, even with this policy setting enabled, anonymous users will have access to resources with permissions that explicitly include the built-in group, **ANONYMOUS LOGON**.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

HKLM\SYSTEM\CurrentControlSet\Control\Lsa:RestrictAnonymous

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow anonymous enumeration of SAM accounts and shares

Default Value:

Disabled. (Allow anonymous enumeration of SAM accounts and shares. No additional permissions can be assigned by the administrator for anonymous connections to the computer. Anonymous connections will rely on default permissions.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.10.5 Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled' (STIG only) (Automated)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting controls the ability of anonymous users to enumerate SAM accounts as well as shares. If you enable this policy setting, anonymous users will not be able to enumerate domain account user names and network share names on the systems in your environment.

The recommended STIG state for this setting is: **Enabled**.

The recommended CIS state for this setting is: **Enabled** on Member Servers only.

Note: This policy has no effect on Domain Controllers.

Rationale:

An unauthorized user could anonymously list account names and shared resources and use the information to attempt to guess passwords or perform social engineering attacks. (Social engineering attacks try to deceive users in some way to obtain passwords or some form of security information.)

Impact:

It will be impossible to establish trusts with Windows NT 4.0-based domains. Also, client computers that run older versions of the Windows operating system such as Windows NT 3.51 and Windows 95 will experience problems when they try to use resources on the server. Users who access file and print servers anonymously will be unable to list the shared network resources on those servers; the users will have to authenticate before they can view the lists of shared folders and printers. However, even with this policy setting enabled, anonymous users will have access to resources with permissions that explicitly include the built-in group, **ANONYMOUS LOGON**.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa:RestrictAnonymous
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow anonymous enumeration of SAM accounts and shares
```

Default Value:

Disabled. (Allow anonymous enumeration of SAM accounts and shares. No additional permissions can be assigned by the administrator for anonymous connections to the computer. Anonymous connections will rely on default permissions.)

Additional Information:

```
Microsoft Windows Server 2016 Security Technical Implementation Guide:  
Version 2, Release 8, Benchmark Date: May 15, 2024
```

```
Vul ID:    V-225046  
Rule ID:   SV-225046r569186_rule  
STIG ID:   WN16-SO-000270  
Severity:  CAT II
```

2.3.10.6 Ensure 'Network access: Do not allow storage of passwords and credentials for network authentication' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting determines whether Credential Manager (formerly called Stored User Names and Passwords) saves passwords or credentials for later use when it gains domain authentication.

The recommended state for this setting is: **Enabled**.

Note: Changes to this setting will not take effect until Windows is restarted.

Rationale:

Passwords that are cached can be accessed by the user when logged on to the computer. Although this information may sound obvious, a problem can arise if the user unknowingly executes hostile code that reads the passwords and forwards them to another, unauthorized user.

Impact:

Credential Manager will not store passwords and credentials on the computer. Users will be forced to enter passwords whenever they log on to their Passport account or other network resources that aren't accessible to their domain account. Testing has shown that clients running Windows Vista or Windows Server 2008 will be unable to connect to Distributed File System (DFS) shares in untrusted domains. Enabling this setting also makes it impossible to specify alternate credentials for scheduled tasks, this can cause a variety of problems. For example, some third-party backup products will no longer work. This policy setting should have no impact on users who access network resources that are configured to allow access with their Active Directory-based domain account.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SYSTEM\CurrentControlSet\Control\Lsa:disableDomainCreds
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow storage of passwords and credentials for network authentication
```

Default Value:

Disabled. (Credential Manager will store passwords and credentials on the computer for later use for domain authentication.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.10.7 Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting determines what additional permissions are assigned for anonymous connections to the computer.

The recommended state for this setting is: **Disabled**.

Rationale:

An unauthorized user could anonymously list account names and shared resources and use the information to attempt to guess passwords, perform social engineering attacks, or launch DoS attacks.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SYSTEM\CurrentControlSet\Control\Lsa:EveryoneIncludesAnonymous
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Let Everyone permissions apply to anonymous users
```

Default Value:

Disabled. (Anonymous users can only access those resources for which the built-in group **ANONYMOUS LOGON** has been explicitly given permission.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225047
Rule ID: SV-225047r569186_rule
STIG ID: WN16-SO-000290
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.10.8 Configure 'Network access: Named Pipes that can be accessed anonymously' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This policy setting determines which communication sessions, or pipes, will have attributes and permissions that allow anonymous access.

The recommended state for this setting is: **LSARPC**, **NETLOGON**, **SAMR** and (when the legacy *Computer Browser* service is enabled) **BROWSER**.

Note: A Member Server that holds the *Remote Desktop Services* Role with *Remote Desktop Licensing* Role Service will require a special exception to this recommendation, to allow the **HydraLSPipe** and **TermServLicensing** Named Pipes to be accessed anonymously.

Rationale:

Limiting named pipes that can be accessed anonymously will reduce the attack surface of the system.

Impact:

Null session access over named pipes will be disabled unless they are included, and applications that rely on this feature or on unauthenticated access to named pipes will no longer function. The **BROWSER** named pipe may need to be added to this list if the *Computer Browser* service is needed for supporting legacy components. The *Computer Browser* service is disabled by default.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_MULTI_SZ** value of **LSARPC, NETLOGON, SAMR**.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters: NullSessionPipes

Remediation:

To establish the recommended configuration via GP, configure the following UI path:

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Named Pipes that can be accessed anonymously

Default Value:

None.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.10.9 Configure 'Network access: Named Pipes that can be accessed anonymously' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy setting determines which communication sessions, or pipes, will have attributes and permissions that allow anonymous access.

The recommended state for this setting is: **<blank>** (i.e. None), or (when the legacy *Computer Browser* service is enabled) **BROWSER**.

Note: A Member Server that holds the *Remote Desktop Services* Role with *Remote Desktop Licensing* Role Service will require a special exception to this recommendation, to allow the **HydraLSPipe** and **TermServLicensing** Named Pipes to be accessed anonymously.

Rationale:

Limiting named pipes that can be accessed anonymously will reduce the attack surface of the system.

Impact:

Null session access over named pipes will be disabled unless they are included, and applications that rely on this feature or on unauthenticated access to named pipes will no longer function. The **BROWSER** named pipe may need to be added to this list if the *Computer Browser* service is needed for supporting legacy components. The *Computer Browser* service is disabled by default.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_MULTI_SZ** value of **0**.

```
HKLM\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters:NullSessionPipes
```

Remediation:

To establish the recommended configuration via GP, configure the following UI path:

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Named Pipes that can be accessed anonymously

Default Value:

None.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.10.10 Configure 'Network access: Remotely accessible registry paths' is configured (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which registry paths will be accessible over the network, regardless of the users or groups listed in the access control list (ACL) of the **winreg** registry key.

Note: This setting does not exist in Windows XP. There was a setting with that name in Windows XP, but it is called "Network access: Remotely accessible registry paths and sub-paths" in Windows Server 2003, Windows Vista, and Windows Server 2008 (non-R2).

Note #2: When you configure this setting you specify a list of one or more objects. The delimiter used when entering the list is a line feed or carriage return, that is, type the first object on the list, press the Enter button, type the next object, press Enter again, etc. The setting value is stored as a comma-delimited list in group policy security templates. It is also rendered as a comma-delimited list in Group Policy Editor's display pane and the Resultant Set of Policy console. It is recorded in the registry as a line-feed delimited list in a REG_MULTI_SZ value.

The recommended state for this setting is:

```
System\CurrentControlSet\Control\ProductOptions  
System\CurrentControlSet\Control\Server Applications  
Software\Microsoft\Windows NT\CurrentVersion
```

Rationale:

The registry is a database that contains computer configuration information, and much of the information is sensitive. An attacker could use this information to facilitate unauthorized activities. To reduce the risk of such an attack, suitable ACLs are assigned throughout the registry to help protect it from access by unauthorized users.

Impact:

None - this is the default behavior. However, if you remove the default registry paths from the list of accessible ones, remote management tools such as the Microsoft Baseline Security Analyzer and Microsoft Systems Management Server could fail, as they require remote access to the registry to properly monitor and manage computers.

Note: If you want to allow remote access, you must also enable the Remote Registry service.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a REG_MULTI_SZ value of

System\CurrentControlSet\Control\ProductOptions, System\CurrentControlSet\Control\Server Applications, Software\Microsoft\Windows NT\CurrentVersion.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\Winreg\AllowedExactPaths:Machine
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to:

System\CurrentControlSet\Control\ProductOptions
System\CurrentControlSet\Control\Server Applications
Software\Microsoft\Windows NT\CurrentVersion

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Remotely accessible registry paths
```

Default Value:

System\CurrentControlSet\Control\ProductOptions
System\CurrentControlSet\Control\Server Applications Software\Microsoft\Windows NT\CurrentVersion

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.10.11 Configure 'Network access: Remotely accessible registry paths and sub-paths' is configured (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which registry paths and sub-paths will be accessible over the network, regardless of the users or groups listed in the access control list (ACL) of the **winreg** registry key.

Note: In Windows XP this setting is called "Network access: Remotely accessible registry paths," the setting with that same name in Windows Vista, Windows Server 2008 (non-R2), and Windows Server 2003 does not exist in Windows XP.

Note #2: When you configure this setting you specify a list of one or more objects. The delimiter used when entering the list is a line feed or carriage return, that is, type the first object on the list, press the Enter button, type the next object, press Enter again, etc. The setting value is stored as a comma-delimited list in group policy security templates. It is also rendered as a comma-delimited list in Group Policy Editor's display pane and the Resultant Set of Policy console. It is recorded in the registry as a line-feed delimited list in a REG_MULTI_SZ value.

The recommended state for this setting is:

```
System\CurrentControlSet\Control\Print\Printers
System\CurrentControlSet\Services\Eventlog
Software\Microsoft\OLAP Server
Software\Microsoft\Windows NT\CurrentVersion\Print
Software\Microsoft\Windows NT\CurrentVersion\Windows
System\CurrentControlSet\Control\ContentIndex
System\CurrentControlSet\Control\Terminal Server
System\CurrentControlSet\Control\Terminal Server\UserConfig
System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration
Software\Microsoft\Windows NT\CurrentVersion\Perflib
System\CurrentControlSet\Services\SysmonLog
```

The recommended state for servers that hold the *Active Directory Certificate Services* Role with *Certification Authority* Role Service includes the above list and:

```
System\CurrentControlSet\Services\CertSvc
```

The recommended state for servers that have the *WINS* Server Feature installed includes the above list and:

```
System\CurrentControlSet\Services\WINS
```

Rationale:

The registry contains sensitive computer configuration information that could be used by an attacker to facilitate unauthorized activities. The fact that the default ACLs assigned throughout the registry are fairly restrictive and help to protect the registry from access by unauthorized users reduces the risk of such an attack.

Impact:

None - this is the default behavior. However, if you remove the default registry paths from the list of accessible ones, remote management tools such as the Microsoft Baseline Security Analyzer and Microsoft Systems Management Server could fail, as they require remote access to the registry to properly monitor and manage computers.

Note: If you want to allow remote access, you must also enable the Remote Registry service.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_MULTI_SZ** value of

```
System\CurrentControlSet\Control\Print\Printers, System\CurrentControlSet\Services\Eventlog, Software\Microsoft\OLAP Server, Software\Microsoft\Windows NT\CurrentVersion\Print, Software\Microsoft\Windows NT\CurrentVersion\Windows, System\CurrentControlSet\Control\ContentIndex, System\CurrentControlSet\Control\Terminal Server, System\CurrentControlSet\Control\Terminal Server\UserConfig, System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration, Software\Microsoft\Windows NT\CurrentVersion\Perflib, System\CurrentControlSet\Services\SysmonLog, System\CurrentControlSet\Services\CertSvc, System\CurrentControlSet\Services\WINS.
```

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\Winreg\
AllowedPaths:Machine
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to:

```
System\CurrentControlSet\Control\Print\Printers
System\CurrentControlSet\Services\Eventlog
Software\Microsoft\OLAP Server
Software\Microsoft\Windows NT\CurrentVersion\Print
Software\Microsoft\Windows NT\CurrentVersion\Windows
System\CurrentControlSet\Control\ContentIndex
System\CurrentControlSet\Control\Terminal Server
System\CurrentControlSet\Control\Terminal Server\UserConfig
System\CurrentControlSet\Control\Terminal
Server\DefaultUserConfiguration
Software\Microsoft\Windows NT\CurrentVersion\Perflib
System\CurrentControlSet\Services\SysmonLog
```

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network access: Remotely accessible registry paths
and sub-paths
```

When a server holds the *Active Directory Certificate Services* Role with *Certification Authority* Role Service, the above list should also include:

```
System\CurrentControlSet\Services\CertSvc.
```

When a server has the *WINS* Server Feature installed, the above list should also include:

```
System\CurrentControlSet\Services\WINS
```

Default Value:

```
System\CurrentControlSet\Control\Print\Printers
System\CurrentControlSet\Services\Eventlog
Software\Microsoft\OLAP Server
Software\Microsoft\Windows NT\CurrentVersion\Print
Software\Microsoft\Windows NT\CurrentVersion\Windows
System\CurrentControlSet\Control\ContentIndex
System\CurrentControlSet\Control\Terminal Server
System\CurrentControlSet\Control\Terminal Server\UserConfig
System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration
Software\Microsoft\Windows NT\CurrentVersion\Perflib
System\CurrentControlSet\Services\SysmonLog
```


CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.10.12 Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

When enabled, this policy setting restricts anonymous access to only those shares and pipes that are named in the **Network access: Named pipes that can be accessed anonymously** and **Network access: Shares that can be accessed anonymously** settings. This policy setting controls null session access to shares on your computers by adding **RestrictNullSessAccess** with the value **1** in the

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters

registry key. This registry value toggles null session shares on or off to control whether the server service restricts unauthenticated clients' access to named resources.

The recommended state for this setting is: **Enabled**.

Rationale:

Null sessions are a weakness that can be exploited through shares (including the default shares) on computers in your environment.

Impact:

None - this is the default behavior. If you choose to enable this setting and are supporting Windows NT 4.0 domains, you should check if any of the named pipes are required to maintain trust relationships between the domains, and then add the pipe to the **Network access: Named pipes that can be accessed anonymously** list:

- COMNAP: SNA session access
- COMNODE: SNA session access
- SQL\QUERY: SQL instance access
- SPOOLSS: Spooler service
- LLSRPC: License Logging service
- NETLOGON: Net Logon service
- LSARPC: LSA access
- SAMR: Remote access to SAM objects
- BROWSER: Computer Browser service

Previous to the release of Windows Server 2003 with Service Pack 1 (SP1) these named pipes were allowed anonymous access by default, but with the increased hardening in Windows Server 2003 with SP1 these pipes must be explicitly added if needed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters:RestrictNullSessionAccess
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Restrict anonymous access to Named Pipes and Shares
```

Default Value:

Enabled. (Anonymous access is restricted to shares and pipes listed in the **Network access: Named pipes that can be accessed anonymously** and **Network access: Shares that can be accessed anonymously** settings.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225048
Rule ID: SV-225048r569186_rule
STIG ID: WN16-SO-000300
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.10.13 Ensure 'Network access: Restrict clients allowed to make remote calls to SAM' is set to 'Administrators: Remote Access: Allow' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server
- STIG Member Server

Description:

This policy setting allows you to restrict remote RPC connections to SAM.

The recommended state for this setting is: **Administrators: Remote Access: Allow**.

Note: A Windows 10 R1607, Server 2016 or newer OS is required to access and set this value in Group Policy.

Note #2: This setting was originally only supported on Windows Server 2016 or newer, then support for it was added to Windows Server 2008 R2 or newer via the March 2017 security patches.

Note #3: If your organization is using Microsoft Defender for Identity (formerly Azure Advanced Threat Protection (Azure ATP)), the (organization-named) Defender for Identity Directory Service Account (DSA), will also need to be granted the same **Remote Access: Allow** permission. For more information on adding the service account please see [Configure SAM-R to enable lateral movement path detection in Microsoft Defender for Identity | Microsoft Docs](#).

Rationale:

To ensure that an unauthorized user cannot anonymously list local account names or groups and use the information to attempt to guess passwords or perform social engineering attacks. (Social engineering attacks try to deceive users in some way to obtain passwords or some form of security information.)

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a REG_SZ value of **O:BAG:BAD:(A;;RC;;;BA)**.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa:restrictremotesam
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Administrators: Remote Access: Allow**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Restrict clients allowed to make remote calls to SAM
```

Default Value:

Administrators: Remote Access: Allow.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225013
Rule ID: SV-225013r877392_rule
STIG ID: WN16-MS-000310
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.10.14 Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which network shares can be accessed by anonymous users. The default configuration for this policy setting has little effect because all users have to be authenticated before they can access shared resources on the server.

The recommended state for this setting is: **<blank>** (i.e. None).

Rationale:

It is very dangerous to allow any values in this setting. Any shares that are listed can be accessed by any network user, which could lead to the exposure or corruption of sensitive data.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_MULTI_SZ** value that is **blank** i.e. no value in key.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters:  
NullSessionShares
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **<blank>** (i.e. None):

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local  
Policies\Security Options\Network access: Shares that can be accessed  
anonymously
```

Default Value:

None. (Only authenticated users will have access to all shared resources on the server.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	14.6 <u>Protect Information through Access Control Lists</u> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

2.3.10.15 Ensure 'Network access: Sharing and security model for local accounts' is set to 'Classic - local users authenticate as themselves' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines how network logons that use local accounts are authenticated. The Classic option allows precise control over access to resources, including the ability to assign different types of access to different users for the same resource. The Guest only option allows you to treat all users equally. In this context, all users authenticate as Guest only to receive the same access level to a given resource.

The recommended state for this setting is: **Classic - local users authenticate as themselves**.

Note: This setting does not affect interactive logons that are performed remotely by using such services as Telnet or Remote Desktop Services (formerly called Terminal Services).

Rationale:

With the Guest only model, any user who can authenticate to your computer over the network does so with guest privileges, which probably means that they will not have write access to shared resources on that computer. Although this restriction does increase security, it makes it more difficult for authorized users to access shared resources on those computers because ACLs on those resources must include access control entries (ACEs) for the Guest account. With the Classic model, local accounts should be password protected. Otherwise, if Guest access is enabled, anyone can use those user accounts to access shared system resources.

Impact:

None - this is the default configuration for domain-joined computers.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SYSTEM\CurrentControlSet\Control\Lsa:ForceGuest
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Classic - local users authenticate as themselves**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Sharing and security model for local accounts
```

Default Value:

On domain-joined computers: Classic - local users authenticate as themselves. (Network logons that use local account credentials authenticate by using those credentials.)

On stand-alone computers: Guest only - local users authenticate as Guest. (Network logons that use local accounts are automatically mapped to the Guest account.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.11 Network security

This section contains recommendations related to network security.

2.3.11.1 Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting determines whether Local System services that use Negotiate when reverting to NTLM authentication can use the computer identity. This policy is supported on at least Windows 7 or Windows Server 2008 R2.

The recommended state for this setting is: **Enabled**.

Rationale:

When connecting to computers running versions of Windows earlier than Windows Vista or Windows Server 2008 (non-R2), services running as Local System and using SPNEGO (Negotiate) that revert to NTLM use the computer identity. In Windows 7, if you are connecting to a computer running Windows Server 2008 or Windows Vista, then a system service uses either the computer identity or a NULL session. When connecting with a NULL session, a system-generated session key is created, which provides no protection but allows applications to sign and encrypt data without errors. When connecting with the computer identity, both signing and encryption is supported in order to provide data protection.

Impact:

Services running as Local System that use Negotiate when reverting to NTLM authentication will use the computer identity. This might cause some authentication requests between Windows operating systems to fail and log an error.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SYSTEM\CurrentControlSet\Control\Lsa:UseMachineId
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Allow Local System to use computer identity for NTLM
```

Default Value:

Disabled. (Services running as Local System that use Negotiate when reverting to NTLM authentication will authenticate anonymously.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225049
Rule ID: SV-225049r569186_rule
STIG ID: WN16-SO-000320
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.11.2 Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting determines whether NTLM is allowed to fall back to a NULL session when used with LocalSystem.

The recommended state for this setting is: **Disabled**.

Rationale:

NULL sessions are less secure because by definition they are unauthenticated.

Impact:

Any applications that require NULL sessions for LocalSystem will not work as designed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0:AllowNullSessionFallback
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Allow LocalSystem NULL session fallback
```

Default Value:

On Windows Server 2008 (non-R2): Enabled. (NTLM will be permitted to fall back to a NULL session when used with LocalSystem.)

On Windows Server 2008 R2 or newer: Disabled. (NTLM will not be permitted to fall back to a NULL session when used with LocalSystem.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225050
Rule ID: SV-225050r569186_rule
STIG ID: WN16-SO-000330
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.11.3 Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This setting determines if online identities are able to authenticate to this computer.

The Public Key Cryptography Based User-to-User (PKU2U) protocol introduced in Windows 7 and Windows Server 2008 R2 is implemented as a security support provider (SSP). The SSP enables peer-to-peer authentication, particularly through the Windows 7 media and file sharing feature called HomeGroup, which permits sharing between computers that are not members of a domain.

With PKU2U, a new extension was introduced to the Negotiate authentication package, **Spnego.dll**. In previous versions of Windows, Negotiate decided whether to use Kerberos or NTLM for authentication. The extension SSP for Negotiate, **Negoexts.dll**, which is treated as an authentication protocol by Windows, supports Microsoft SSPs including PKU2U.

When computers are configured to accept authentication requests by using online IDs, **Negoexts.dll** calls the PKU2U SSP on the computer that is used to log on. The PKU2U SSP obtains a local certificate and exchanges the policy between the peer computers. When validated on the peer computer, the certificate within the metadata is sent to the logon peer for validation and associates the user's certificate to a security token and the logon process completes.

The recommended state for this setting is: **Disabled**.

Note: If a hybrid environment is used, and PKU2U is **Disabled**, Remote Desktop connections from a hybrid joined system to a hybrid joined system will fail.

Rationale:

The PKU2U protocol is a peer-to-peer authentication protocol - authentication should be managed centrally in most managed networks.

Impact:

None - this is the default configuration for domain-joined computers.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SYSTEM\CurrentControlSet\Control\Lsa\pku2u:AllowOnlineID
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network Security: Allow PKU2U authentication requests to this computer to use online identities
```

Default Value:

Disabled. (Online identities will not to be allowed to authenticate to a domain-joined machine.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225051
Rule ID: SV-225051r569186_rule
STIG ID: WN16-SO-000340
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.			

2.3.11.4 Ensure 'Network security: Configure encryption types allowed for Kerberos' is set to 'AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting allows you to set the encryption types that Kerberos is allowed to use.

The recommended state for this setting is: **AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types**.

Note: Some legacy applications and OSes may still require **RC4_HMAC_MD5** - we recommend you test in your environment and verify whether you can safely remove it.

Rationale:

The strength of each encryption algorithm varies from one to the next, choosing stronger algorithms will reduce the risk of compromise however doing so may cause issues when the computer attempts to authenticate with systems that do not support them.

Impact:

If not selected, the encryption type will not be allowed. This setting may affect compatibility with client computers or services and applications. Multiple selections are permitted.

Note: Some legacy applications and OSes may still require **RC4_HMAC_MD5** - we recommend you test in your environment and verify whether you can safely remove it.

Note #2: Windows Server 2008 (non-R2) and below allow DES for Kerberos by default, but later OS versions do not.

Note #3: Some prerequisites might need to be met on Domain Controllers to support Kerberos AES 128 and 256 bit encryption types, as well as enabling support for Kerberos AES 128 and 256 bit on user accounts (in account options) for this recommendation to work correctly.

Note #4: If your organization uses Azure Files, please note that Microsoft did not introduce AES 256 Kerberos encryption support for it until AD DS authentication module v0.2.2. Please see this link for more information:

[Azure Files on-premises AD DS Authentication support for AES 256 Kerberos encryption | Microsoft Docs](#)

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **2147483640**.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Kerberos\Parameters:SupportedEncryptionTypes
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Configure encryption types allowed for Kerberos
```

Default Value:

RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225052
Rule ID: SV-225052r569186_rule
STIG ID: WN16-SO-000350
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.			
v7	18.5 <u>Use Only Standardized and Extensively Reviewed Encryption Algorithms</u> Use only standardized and extensively reviewed encryption algorithms.			

2.3.11.5 Ensure 'Network security: Do not store LAN Manager hash value on next password change' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting determines whether the LAN Manager (LM) hash value for the new password is stored when the password is changed. The LM hash is relatively weak and prone to attack compared to the cryptographically stronger Microsoft Windows NT hash. Since LM hashes are stored on the local computer in the security database, passwords can then be easily compromised if the database is attacked.

Note: Older operating systems and some third-party applications may fail when this policy setting is enabled. Also, note that the password will need to be changed on all accounts after you enable this setting to gain the proper benefit.

The recommended state for this setting is: **Enabled**.

Rationale:

The SAM file can be targeted by attackers who seek access to username and password hashes. Such attacks use special tools to crack passwords, which can then be used to impersonate users and gain access to resources on your network. These types of attacks will not be prevented if you enable this policy setting, but it will be much more difficult for these types of attacks to succeed.

Impact:

None - this is the default behavior. Earlier operating systems such as Windows 95, Windows 98, and Windows ME as well as some third-party applications will fail.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SYSTEM\CurrentControlSet\Control\Lsa:NoLMHash
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Do not store LAN Manager hash value on next password change
```

Default Value:

Enabled. (LAN Manager hash values are not stored when passwords are changed.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225053
Rule ID: SV-225053r877397_rule
STIG ID: WN16-SO-000360
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 <u>Encrypt Sensitive Data at Rest</u> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
v7	16.4 <u>Encrypt or Hash all Authentication Credentials</u> Encrypt or hash with a salt all authentication credentials when stored.			

2.3.11.6 Ensure 'Network security: Force logoff when logon hours expire' is set to 'Enabled' (Manual)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether to disconnect users who are connected to the local computer outside their user account's valid logon hours. This setting affects the Server Message Block (SMB) component. If you enable this policy setting you should also enable *Microsoft network server: Disconnect clients when logon hours expire* (Rule 2.3.9.4).

The recommended state for this setting is: **Enabled**.

Rationale:

If this setting is disabled, a user could remain connected to the computer outside of their allotted logon hours.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**.

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Force logoff when logon hours expire
```

Default Value:

Enabled. (When a user's logon time expires, client sessions with the SMB server will be forcibly disconnected. The user will be unable to log on to the computer until their next scheduled access time commences.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	16.13 <u>Alert on Account Login Behavior Deviation</u> Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

2.3.11.7 Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

LAN Manager (LM) was a family of early Microsoft client/server software (predating Windows NT) that allowed users to link personal computers together on a single network. LM network capabilities included transparent file and print sharing, user security features, and network administration tools. In Active Directory domains, the Kerberos protocol is the default authentication protocol. However, if the Kerberos protocol is not negotiated for some reason, Active Directory will use LM, NTLM, or NTLMv2. LAN Manager authentication includes the LM, NTLM, and NTLM version 2 (NTLMv2) variants, and is the protocol that is used to authenticate all Windows clients when they perform the following operations:

- Join a domain
- Authenticate between Active Directory forests
- Authenticate to down-level domains
- Authenticate to computers that do not run Windows 2000, Windows Server 2003, or Windows XP
- Authenticate to computers that are not in the domain

The Network security: LAN Manager authentication level setting determines which challenge/response authentication protocol is used for network logons. This choice affects the level of authentication protocol used by clients, the level of session security negotiated, and the level of authentication accepted by servers.

The recommended state for this setting is: **Send NTLMv2 response only. Refuse LM & NTLM.**

Rationale:

Windows 2000 and Windows XP clients were configured by default to send LM and NTLM authentication responses (Windows 95-based and Windows 98-based clients only send LM). The default settings in OSes predating Windows Vista / Windows Server 2008 (non-R2) allowed all clients to authenticate with servers and use their resources. However, this meant that LM responses - the weakest form of authentication response - were sent over the network, and it was potentially possible for attackers to sniff that traffic to more easily reproduce the user's password.

The Windows 95, Windows 98, and Windows NT operating systems cannot use the Kerberos version 5 protocol for authentication. For this reason, in a Windows Server 2003 domain, these computers authenticate by default with both the LM and NTLM protocols for network authentication. You can enforce a more secure authentication protocol for Windows 95, Windows 98, and Windows NT by using NTLMv2. For the logon process, NTLMv2 uses a secure channel to protect the authentication process. Even if you use NTLMv2 for older clients and servers, Windows-based clients and servers that are members of the domain will use the Kerberos authentication protocol to authenticate with Windows Server 2003 or newer Domain Controllers. For these reasons, it is strongly preferred to restrict the use of LM & NTLM (non-v2) as much as possible.

Impact:

Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it; Domain Controllers refuse LM and NTLM (accept only NTLMv2 authentication). Clients that do not support NTLMv2 authentication will not be able to authenticate in the domain and access domain resources by using LM and NTLM.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **5**.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa:LmCompatibilityLevel
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to: **Send NTLMv2 response only. Refuse LM & NTLM:**

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: LAN Manager authentication level
```

Default Value:

Send NTLMv2 response only. (Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it; Domain Controllers accept LM, NTLM & NTLMv2 authentication.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225054
Rule ID: SV-225054r857283_rule
STIG ID: WN16-SO-000380
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	18.5 <u>Use Only Standardized and Extensively Reviewed Encryption Algorithms</u> Use only standardized and extensively reviewed encryption algorithms.			

2.3.11.8 Ensure 'Network security: LDAP client signing requirements' is set to 'Negotiate signing' or higher (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting determines the level of data signing that is requested on behalf of clients that issue LDAP BIND requests.

Note: This policy setting does not have any impact on LDAP simple bind (`ldap_simple_bind`) or LDAP simple bind through SSL (`ldap_simple_bind_s`). No Microsoft LDAP clients that are included with Windows XP Professional use `ldap_simple_bind` or `ldap_simple_bind_s` to communicate with a Domain Controller.

The recommended state for this setting is: **Negotiate signing**. Configuring this setting to **Require signing** also conforms to the benchmark.

Rationale:

Unsigned network traffic is susceptible to man-in-the-middle attacks in which an intruder captures the packets between the client and server, modifies them, and then forwards them to the server. For an LDAP server, this susceptibility means that an attacker could cause a server to make decisions that are based on false or altered data from the LDAP queries. To lower this risk in your network, you can implement strong physical security measures to protect the network infrastructure. Also, you can make all types of man-in-the-middle attacks extremely difficult if you require digital signatures on all network packets by means of IPsec authentication headers.

Impact:

None - this is the default behavior. However, if you choose instead to configure the server to *require* LDAP signatures then you must also configure the client. If you do not configure the client it will not be able to communicate with the server, which could cause many features to fail, including user authentication, Group Policy, and logon scripts, because the caller will be told that the LDAP BIND command request failed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

HKLM\SYSTEM\CurrentControlSet\Services\LDAP:LDAPClientIntegrity

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Negotiate signing** (configuring to **Require signing** also conforms to the benchmark):

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: LDAP client signing requirements

Default Value:

Negotiate signing. (If Transport Layer Security/Secure Sockets Layer (TLS/SSL) has not been started, the LDAP BIND request is initiated with the LDAP data signing option set in addition to the caller-specified options. If TLS/SSL has been started, the LDAP BIND request is initiated with the caller-specified options.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225055
Rule ID: SV-225055r569186_rule
STIG ID: WN16-SO-000390
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	18.5 <u>Use Only Standardized and Extensively Reviewed Encryption Algorithms</u> Use only standardized and extensively reviewed encryption algorithms.			

2.3.11.9 Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit encryption' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting determines which behaviors are allowed by clients for applications using the NTLM Security Support Provider (SSP). The SSP Interface (SSPI) is used by applications that need authentication services. The setting does not modify how the authentication sequence works but instead require certain behaviors in applications that use the SSPI.

The recommended state for this setting is: **Require NTLMv2 session security, Require 128-bit encryption.**

Note: These values are dependent on the *Network security: LAN Manager Authentication Level* (Rule 2.3.11.7) security setting value.

Rationale:

You can enable both options for this policy setting to help protect network traffic that uses the NTLM Security Support Provider (NTLM SSP) from being exposed or tampered with by an attacker who has gained access to the same network. In other words, these options help protect against man-in-the-middle attacks.

Impact:

NTLM connections will fail if NTLMv2 protocol and strong encryption (128-bit) are not **both** negotiated. Client applications that are enforcing these settings will be unable to communicate with older servers that do not support them.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **537395200**.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0:NTLMMinClientSec
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Require NTLMv2 session security, Require 128-bit encryption**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Minimum session security for NTLM SSP based (including secure RPC) clients
```

Default Value:

On Windows Server 2008 (non-R2): No requirements.

On Windows Server 2008 R2 or newer: Require 128-bit encryption. (NTLM connections will fail if strong encryption (128-bit) is not negotiated.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225056
Rule ID: SV-225056r569186_rule
STIG ID: WN16-SO-000400
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	18.5 <u>Use Only Standardized and Extensively Reviewed Encryption Algorithms</u> Use only standardized and extensively reviewed encryption algorithms.			

2.3.11.10 Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting determines which behaviors are allowed by servers for applications using the NTLM Security Support Provider (SSP). The SSP Interface (SSPI) is used by applications that need authentication services. The setting does not modify how the authentication sequence works but instead require certain behaviors in applications that use the SSPI.

The recommended state for this setting is: **Require NTLMv2 session security, Require 128-bit encryption.**

Note: These values are dependent on the *Network security: LAN Manager Authentication Level* (Rule 2.3.11.7) security setting value.

Rationale:

You can enable all of the options for this policy setting to help protect network traffic that uses the NTLM Security Support Provider (NTLM SSP) from being exposed or tampered with by an attacker who has gained access to the same network. That is, these options help protect against man-in-the-middle attacks.

Impact:

NTLM connections will fail if NTLMv2 protocol and strong encryption (128-bit) are not **both** negotiated. Server applications that are enforcing these settings will be unable to communicate with older servers that do not support them.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **537395200**.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0:NtlmMinServerSec
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Require NTLMv2 session security, Require 128-bit encryption**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Minimum session security for NTLM SSP based (including secure RPC) servers
```

Default Value:

On Windows Server 2008 (non-R2): No requirements.

On Windows Server 2008 R2 or newer: Require 128-bit encryption. (NTLM connections will fail if strong encryption (128-bit) is not negotiated.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225057
Rule ID: SV-225057r569186_rule
STIG ID: WN16-SO-000410
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	18.5 <u>Use Only Standardized and Extensively Reviewed Encryption Algorithms</u> Use only standardized and extensively reviewed encryption algorithms.			

2.3.11.11 Ensure 'Network security: Restrict NTLM: Audit Incoming NTLM Traffic' is set to 'Enable auditing for all accounts' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows the auditing of incoming NTLM traffic. Events for this setting are recorded in the operational event log (e.g. Applications and Services Log\Microsoft\Windows\NTLM).

The recommended state for this setting is: **Enable auditing for all accounts**.

Rationale:

Auditing and monitoring NTLM traffic can assist in identifying systems using this outdated authentication protocol, so they can be remediated to using a more secure protocol, such as Kerberos. The log information gathered can also assist in forensic investigations after a malicious attack.

NTLM and NTLMv2 authentication is vulnerable to various attacks, including SMB relay, man-in-the-middle, and brute force attacks. Reducing and eliminating NTLM authentication in an environment reduces the risk of an attacker gaining access to systems on the network.

Impact:

The event log will contain information on incoming NTLM authentication traffic.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **2**.

```
HKLM\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0:AuditReceivingNTLMTraffic
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enable auditing for all accounts**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Restrict NTLM: Audit Incoming NTLM Traffic
```

Default Value:

Disabled. (Incoming NTLM traffic is not logged.)

References:

1. <https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-restrict-ntlm-audit-incoming-ntlm-traffic>
2. <https://learn.microsoft.com/en-us/defender-for-identity/configure-windows-event-collection#event-id-8004>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			

2.3.11.12 Ensure 'Network security: Restrict NTLM: Audit NTLM authentication in this domain' is set to 'Enable all' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This policy setting allows auditing of NTLM authentication within the domain from the Domain Controller.

The recommended state for this setting is: **Enable all**.

Note: This setting is specific to each Domain Controller and will only log authentications made to that Domain Controller.

Rationale:

Auditing and monitoring NTLM traffic can assist in identifying systems using this outdated authentication protocol, so they can be remediated to using a more secure protocol, such as Kerberos. The log information gathered can also assist in forensic investigations after a malicious attack.

NTLM and NTLMv2 authentication is vulnerable to various attacks, including SMB relay, man-in-the-middle, and brute force attacks. Reducing and eliminating NTLM authentication in an environment reduces the risk of an attacker gaining access to systems on the network.

Impact:

The event log will contain information on NTLM authentication traffic made to that Domain Controller.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **7**.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters:AuditNTLMInDomain
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enable all**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Restrict NTLM: Audit NTLM authentication in this domain
```

Default Value:

Disabled. (The domain controller will not log events for NTLM authentication in this domain.)

References:

1. <https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-restrict-ntlm-audit-ntlm-authentication-in-this-domain>
2. <https://learn.microsoft.com/en-us/defender-for-identity/what-is>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			

2.3.11.13 Ensure 'Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers' is set to 'Audit all' or higher (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows the auditing of outgoing NTLM traffic. Events for this setting are recorded in the operational event log (e.g. Applications and Services Log\Microsoft\Windows\NTLM).

The recommended state for this setting is: **Audit all**. Configuring this setting to **Deny All** also conforms to the benchmark.

Note: Configuring this setting to **Deny All** is more secure, however it could have a negative impact on applications that still require NTLM. Test carefully before implementing the **Deny All** value.

Rationale:

Auditing and monitoring NTLM traffic can assist in identifying systems using this outdated authentication protocol, so they can be remediated to using a more secure protocol, such as Kerberos. The log information gathered can also assist in forensic investigations after a malicious attack.

NTLM and NTLMv2 authentication is vulnerable to various attacks, including SMB relay, man-in-the-middle, and brute force attacks. Reducing and eliminating NTLM authentication in an environment reduces the risk of an attacker gaining access to systems on the network.

Impact:

The event log will contain information on outgoing NTLM authentication traffic.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **2**.

```
HKLM\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0:RestrictSendingNTLMTraffic
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Audit all** or higher:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Restrict NTLM: Outgoing NTLM traffic to remote servers
```

Default Value:

Allow all. (The client can authenticate to remote servers by using NTLM authentication.)

References:

1. <https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-restrict-ntlm-audit-incoming-ntlm-traffic>
2. <https://learn.microsoft.com/en-us/defender-for-identity/configure-windows-event-collection#event-id-8004>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●

2.3.12 Recovery console

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

2.3.13 Shutdown

This section contains recommendations related to the Windows shutdown functionality.

2.3.13.1 Ensure 'Shutdown: Allow system to be shut down without having to log on' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether a computer can be shut down when a user is not logged on. If this policy setting is enabled, the shutdown command is available on the Windows logon screen. It is recommended to disable this policy setting to restrict the ability to shut down the computer to users with credentials on the system.

The recommended state for this setting is: **Disabled**.

Note: In Server 2008 R2 and older versions, this setting had no impact on Remote Desktop (RDP) / Terminal Services sessions - it only affected the local console. However, Microsoft changed the behavior in Windows Server 2012 (non-R2) and above, where if set to Enabled, RDP sessions are also allowed to shut down or restart the server.

Rationale:

Users who can access the console locally could shut down the computer. Attackers could also walk to the local console and restart the server, which would cause a temporary DoS condition. Attackers could also shut down the server and leave all of its applications and services unavailable. As noted in the Description above, the Denial of Service (DoS) risk of enabling this setting dramatically increases in Windows Server 2012 (non-R2) and above, as even remote users could then shut down or restart the server from the logon screen of an RDP session.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:ShutdownWithoutLogon
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Shutdown: Allow system to be shut down without having to log on
```

Default Value:

Disabled. (Operators will have to log on to servers to shut them down or restart them.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.14 System cryptography

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

2.3.14.1 Ensure 'System cryptography: Force strong key protection for user keys stored on the computer' is set to 'User must enter a password each time they use a key' (STIG only) (Automated)

Profile Applicability:

- STIG Member Server
- STIG Domain Controller

Description:

This policy setting determines whether users can use private keys, such as their Secure/Multipurpose Internet Mail Extensions (S/MIME) key, without a password.

The STIG recommended state for this setting is: **User must enter a password each time they use a key.**

Rationale:

If a private key is compromised, an attacker can use the keys that are stored to gain access to the network. If users must provide a password each time they use the key, it will make it more difficult for an attacker to access locally stored keys.

Impact:

A user must provide a password each time they use a key. This is in addition to their domain password.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **2**.

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Cryptography:ForceKeyProtection
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **User must enter a password each time they use a key:**

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\System Cryptography: Force strong key protection for user keys stored on the computer

Default Value:

Not Configured

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225058
Rule ID: SV-225058r569186_rule
STIG ID: WN16-SO-000420
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 <u>Encrypt Sensitive Data at Rest</u> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
v7	16.4 <u>Encrypt or Hash all Authentication Credentials</u> Encrypt or hash with a salt all authentication credentials when stored.			

2.3.14.2 Ensure 'System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing' is set to 'Enabled' (STIG only) (Automated)

Profile Applicability:

- STIG Member Server
- STIG Domain Controller

Description:

This policy setting determines if the Federal Information Processing Standard (FIPS) compliant algorithms for encryption, hashing, and signing are used.

FIPS is a set of security implementation standards that are used for document processing, encryption algorithms and other information technology standards. These standards are used by departments and agencies of the United States federal government.

The STIG recommended state for this setting is: **Enabled**.

Note: For TLS/SSL this setting determines whether the security provider supports only the FIPS-compliant strong cipher suite known as TLS_RSA_WITH_3DES_EDE_CBC_SHA.

Note #2: For the Encrypting File System (EFS) service, this policy setting supports the 3DES and Advanced Encryption Standard (AES) encryption algorithms for encrypting file data supported by the NTFS file system.

Note #3: For Remote Desktop Services (RDP), this policy should only be enabled if the 3DES encryption algorithm is supported.

Note #4: For BitLocker this policy setting needs to be enabled before any encryption key is generated.

Note #5: For more information on this policy setting please visit [System cryptography Use FIPS compliant algorithms for encryption, hashing, and signing \(Windows 10\) - Windows security | Microsoft Docs and FIPS 140 Validation - Windows security | Microsoft Docs](#).

Rationale:

This policy setting ensures that the system uses algorithms that are Federal Information Processing Standard (FIPS) compliant for digital encryption, hashing, and signing.

Impact:

Client devices that have this policy setting enabled will not be able to communicate by means of digitally encrypted or signed protocols with servers that do not support these algorithms. Network clients that do not support these algorithms will not be able to use servers that require them for network communications.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\FIPSAAlgorithmPolicy:Enabled
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing
```

Default Value:

Disabled.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225059
Rule ID: SV-225059r877398_rule
STIG ID: WN16-SO-000430
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v8	3.11 <u>Encrypt Sensitive Data at Rest</u> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
v7	18.5 <u>Use Only Standardized and Extensively Reviewed Encryption Algorithms</u> Use only standardized and extensively reviewed encryption algorithms.			

2.3.15 System objects

This section contains recommendations related to system objects.

2.3.15.1 Ensure 'System objects: Require case insensitivity for non-Windows subsystems' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether case insensitivity is enforced for all subsystems. The Microsoft Win32 subsystem is case insensitive. However, the kernel supports case sensitivity for other subsystems, such as the Portable Operating System Interface for UNIX (POSIX). Because Windows is case insensitive (but the POSIX subsystem will support case sensitivity), failure to enforce this policy setting makes it possible for a user of the POSIX subsystem to create a file with the same name as another file by using mixed case to label it. Such a situation can block access to these files by another user who uses typical Win32 tools, because only one of the files will be available.

The recommended state for this setting is: **Enabled**.

Rationale:

Because Windows is case-insensitive but the POSIX subsystem will support case sensitivity, failure to enable this policy setting would make it possible for a user of that subsystem to create a file with the same name as another file but with a different mix of upper and lower case letters. Such a situation could potentially confuse users when they try to access such files from normal Win32 tools because only one of the files will be available.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SYSTEM\CurrentControlSet\Control\Session  
Manager\Kernel:ObCaseInsensitive
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\System objects: Require case insensitivity for non-Windows subsystems

Default Value:

Enabled. (All subsystems will be forced to observe case insensitivity. This configuration may confuse users who are familiar with any UNIX-based operating systems that is case-sensitive.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.15.2 Ensure 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting determines the strength of the default discretionary access control list (DACL) for objects. Active Directory maintains a global list of shared system resources, such as DOS device names, mutexes, and semaphores. In this way, objects can be located and shared among processes. Each type of object is created with a default DACL that specifies who can access the objects and what permissions are granted.

The recommended state for this setting is: **Enabled**.

Rationale:

This setting determines the strength of the default DACL for objects. Windows maintains a global list of shared computer resources so that objects can be located and shared among processes. Each type of object is created with a default DACL that specifies who can access the objects and with what permissions.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

HKLM\SYSTEM\CurrentControlSet\Control\Session Manager:ProtectionMode

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)
```

Default Value:

Enabled. (The default DACL is stronger, allowing users who are not administrators to read shared objects but not allowing these users to modify shared objects that they did not create.)

Additional Information:

```
Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID:      V-225060
Rule ID:     SV-225060r569186_rule
STIG ID:     WN16-SO-000450
Severity:    CAT II
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			

2.3.16 System settings

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

2.3.17 User Account Control

This section contains recommendations related to User Account Control.

2.3.17.1 Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting controls the behavior of Admin Approval Mode for the built-in Administrator account.

The recommended state for this setting is: **Enabled**.

Rationale:

One of the risks that the User Account Control feature introduced with Windows Vista is trying to mitigate is that of malicious software running under elevated credentials without the user or administrator being aware of its activity. An attack vector for these programs was to discover the password of the account named "Administrator" because that user account was created for all installations of Windows. To address this risk, in Windows Vista or newer, the built-in Administrator account is now disabled by default. In a default installation of a new computer, accounts with administrative control over the computer are initially set up in one of two ways:

- If the computer is not joined to a domain, the first user account you create has the equivalent permissions as a local administrator.
- If the computer is joined to a domain, no local administrator accounts are created. The Enterprise or Domain Administrator must log on to the computer and create one if a local administrator account is warranted.

Once Windows is installed, the built-in Administrator account may be manually enabled, but we strongly recommend that this account remain disabled.

Impact:

The built-in Administrator account uses Admin Approval Mode. Users that log on using the local Administrator account will be prompted for consent whenever a program requests an elevation in privilege, just like any other user would.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:FilterAdministratorToken
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Admin Approval Mode for the Built-in Administrator account
```

Default Value:

Disabled. (The built-in Administrator account runs all applications with full administrative privilege.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225061
Rule ID: SV-225061r852388_rule
STIG ID: WN16-SO-000460
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	4.3 <u>Ensure the Use of Dedicated Administrative Accounts</u> Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●

2.3.17.2 Ensure 'User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop' is set to 'Disabled' (STIG only) (Automated)

Profile Applicability:

- STIG Member Server
- STIG Domain Controller

Description:

This policy setting controls whether User Interface Accessibility (UIAccess or UIA) programs can automatically disable the secure desktop for elevation prompts used by a standard user.

The recommended STIG state for this setting is: **Disabled**.

Rationale:

Standard elevation prompt dialog boxes can be spoofed, which may cause users to disclose their passwords to malicious software. The secure desktop presents a very distinct appearance when prompting for elevation, where the user desktop dims, and the elevation prompt UI is more prominent. This increases the likelihood that users who become accustomed to the secure desktop will recognize a spoofed elevation prompt dialog box and not fall for the trick.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:  
EnableUIADesktopToggle
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local  
Policies\Security Options\User Account Control: Allow UIAccess applications  
to prompt for elevation without using the secure desktop
```

Default Value:

Disabled. (The secure desktop can be disabled only by the user of the interactive desktop or by disabling the User Account Control: Switch to the secure desktop when prompting for elevation policy setting.)

Additional Information:

```
Microsoft Windows Server 2016 Security Technical Implementation Guide:  
Version 2, Release 8, Benchmark Date: May 15, 2024
```

```
Vul ID:    V-225062  
Rule ID:   SV-225062r569186_rule  
STIG ID:   WN16-SO-000470  
Severity:  CAT II
```

2.3.17.3 Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop' or higher (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting controls the behavior of the elevation prompt for administrators.

The recommended state for this setting is: **Prompt for consent on the secure desktop**. Configuring this setting to **Prompt for credentials on the secure desktop** also conforms to the benchmark.

Rationale:

One of the risks that the UAC feature introduced with Windows Vista is trying to mitigate is that of malicious software running under elevated credentials without the user or administrator being aware of its activity. This setting raises awareness to the administrator of elevated privilege operations and permits the administrator to prevent a malicious program from elevating its privilege when the program attempts to do so.

Impact:

When an operation (including execution of a Windows binary) requires elevation of privilege, the user is prompted on the secure desktop to select either Permit or Deny. If the user selects Permit, the operation continues with the user's highest available privilege.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1** or **2**.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:ConsentPromptBehaviorAdmin
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Prompt for consent on the secure desktop** or **Prompt for credentials on the secure desktop**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode
```

Default Value:

Prompt for consent for non-Windows binaries. (When an operation for a non-Microsoft application requires elevation of privilege, the user is prompted on the secure desktop to select either Permit or Deny. If the user selects Permit, the operation continues with the user's highest available privilege.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225063
Rule ID: SV-225063r569186_rule
STIG ID: WN16-SO-000480
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.17.4 Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting controls the behavior of the elevation prompt for standard users.

The recommended state for this setting is: **Automatically deny elevation requests**.

Rationale:

One of the risks that the User Account Control feature introduced with Windows Vista is trying to mitigate is that of malicious programs running under elevated credentials without the user or administrator being aware of their activity. This setting raises awareness to the user that a program requires the use of elevated privilege operations and requires that the user be able to supply administrative credentials in order for the program to run.

Impact:

When an operation requires elevation of privilege, a configurable access denied error message is displayed. An enterprise that is running desktops as standard user may choose this setting to reduce help desk calls.

Note: With this setting configured as recommended, the default error message displayed when a user attempts to perform an operation or run a program requiring privilege elevation (without Administrator rights) is *"This program will not run. This program is blocked by group policy. For more information, contact your system administrator."* Some users who are not used to seeing this message may believe that the operation or program they attempted to run is specifically blocked by group policy, as that is what the message seems to imply. This message may therefore result in user questions as to why that specific operation/program is blocked, when in fact, the problem is that they need to perform the operation or run the program with an Administrative account (or "Run as Administrator" if it is already an Administrator account), and they are not doing that.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:ConsentPromptBehaviorUser
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Automatically deny elevation requests**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Behavior of the elevation prompt for standard users
```

Default Value:

Prompt for credentials. (When an operation requires elevation of privilege, the user is prompted to enter an administrative user name and password. If the user enters valid credentials, the operation continues with the applicable privilege.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225064
Rule ID: SV-225064r852389_rule
STIG ID: WN16-SO-000490
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.17.5 Ensure 'User Account Control: Detect application installations and prompt for elevation' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting controls the behavior of application installation detection for the computer.

The recommended state for this setting is: **Enabled**.

Rationale:

Some malicious software will attempt to install itself after being given permission to run. For example, malicious software with a trusted application shell. The user may have given permission for the program to run because the program is trusted, but if they are then prompted for installation of an unknown component this provides another way of trapping the software before it can do damage

Impact:

When an application installation package is detected that requires elevation of privilege, the user is prompted to enter an administrative user name and password. If the user enters valid credentials, the operation continues with the applicable privilege.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:EnableInstallerDetection
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Detect application installations and prompt for elevation

Default Value:

Disabled. (Default for enterprise. Application installation packages are not detected and prompted for elevation.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225065
Rule ID: SV-225065r569186_rule
STIG ID: WN16-SO-000500
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.17.6 Ensure 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting controls whether applications that request to run with a User Interface Accessibility (UIAccess) integrity level must reside in a secure location in the file system. Secure locations are limited to the following:

- ...\\Program Files\\, including subfolders
- ...\\Windows\\System32\\
- ...\\Program Files (x86)\\, including subfolders (for 64-bit versions of Windows)

Note: Windows enforces a public key infrastructure (PKI) signature check on any interactive application that requests to run with a UIAccess integrity level regardless of the state of this security setting.

The recommended state for this setting is: **Enabled**.

Rationale:

UIAccess Integrity allows an application to bypass User Interface Privilege Isolation (UIPI) restrictions when an application is elevated in privilege from a standard user to an administrator. This is required to support accessibility features such as screen readers that are transmitting user interfaces to alternative forms. A process that is started with UIAccess rights has the following abilities:

- To set the foreground window.
- To drive any application window using SendInput function.
- To use read input for all integrity levels using low-level hooks, raw input, GetKeyState, GetAsyncKeyState, and GetKeyboardInput.
- To set journal hooks.
- To uses AttachThreadInput to attach a thread to a higher integrity input queue.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:EnableSecureUI  
APaths
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local  
Policies\Security Options\User Account Control: Only elevate UIAccess  
applications that are installed in secure locations
```

Default Value:

Enabled. (If an application resides in a secure location in the file system, it runs only with UIAccess integrity.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225066
Rule ID: SV-225066r569186_rule
STIG ID: WN16-SO-000510
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.17.7 Ensure 'User Account Control: Run all administrators in Admin Approval Mode' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting controls the behavior of all User Account Control (UAC) policy settings for the computer. If you change this policy setting, you must restart your computer.

The recommended state for this setting is: **Enabled**.

Note: If this policy setting is disabled, the Security Center notifies you that the overall security of the operating system has been reduced.

Rationale:

This is the setting that turns on or off UAC. If this setting is disabled, UAC will not be used and any security benefits and risk mitigations that are dependent on UAC will not be present on the system.

Impact:

None - this is the default behavior. Users and administrators will need to learn to work with UAC prompts and adjust their work habits to use least privilege operations.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:EnableLUA

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Run all administrators in Admin Approval Mode

Default Value:

Enabled. (Admin Approval Mode is enabled. This policy must be enabled and related UAC policy settings must also be set appropriately to allow the built-in Administrator account and all other users who are members of the Administrators group to run in Admin Approval Mode.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225067
Rule ID: SV-225067r852390_rule
STIG ID: WN16-SO-000520
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.17.8 Ensure 'User Account Control: Switch to the secure desktop when prompting for elevation' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls whether the elevation request prompt is displayed on the interactive user's desktop or the secure desktop.

The recommended state for this setting is: **Enabled**.

Rationale:

Standard elevation prompt dialog boxes can be spoofed, which may cause users to disclose their passwords to malicious software. The secure desktop presents a very distinct appearance when prompting for elevation, where the user desktop dims, and the elevation prompt UI is more prominent. This increases the likelihood that users who become accustomed to the secure desktop will recognize a spoofed elevation prompt dialog box and not fall for the trick.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:PromptOnSecure Desktop
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Switch to the secure desktop when prompting for elevation

Default Value:

Enabled. (All elevation requests go to the secure desktop regardless of prompt behavior policy settings for administrators and standard users.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3.17.9 Ensure 'User Account Control: Virtualize file and registry write failures to per-user locations' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting controls whether application write failures are redirected to defined registry and file system locations. This policy setting mitigates applications that run as administrator and write run-time application data to:

- %ProgramFiles%
- %windir%
- %windir%\System32
- HKEY_LOCAL_MACHINE\SOFTWARE

The recommended state for this setting is: **Enabled**.

Rationale:

This setting reduces vulnerabilities by ensuring that legacy applications only write data to permitted locations.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:EnableVirtualization
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Virtualize file and registry write failures to per-user locations

Default Value:

Enabled. (Application write failures are redirected at run time to defined user locations for both the file system and registry.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225068
Rule ID: SV-225068r569186_rule
STIG ID: WN16-SO-000530
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

3 Event Log

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

4 Restricted Groups

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

5 System Services

This section contains recommendations for system services.

5.1 Ensure 'Microsoft FTP Service (FTPSVC)' is set to 'Not Installed' (STIG only) (Automated)

Profile Applicability:

- STIG Member Server
- STIG Domain Controller

Description:

This policy setting enables the server to be a File Transfer Protocol (FTP) server.

The STIG recommended state for this setting is: **Not Installed**.

Note: This service is not installed by default. It is supplied with Windows, but is installed by enabling an optional Windows feature (*Internet Information Services - FTP Server*).

Rationale:

Hosting an FTP server (especially a non-secure FTP server) from a workstation is an increased security risk, as the attack surface of that workstation is then greatly increased.

Note: This security concern applies to any FTP server application installed on a workstation, not just IIS.

Impact:

The computer will not function as an FTP server.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location and when set properly a **REG_DWORD** value **does not exist**.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\FTPSVC:Start

Note: Alternately this Windows Feature can be uninstalled by using *Roles and Features* in Server Manager.

Remediation:

To establish the recommended configuration via GP, set the following UI path to: **Not Installed**.

Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Microsoft FTP Service

OR

To Uninstall the *FTP Server* role:

- Start *Server Manager*
- Select the server with the role
- Scroll down to *ROLES AND FEATURES* in the right pane
- Select *Remove Roles and Features* from the drop-down *TASKS* list
- Select the appropriate server on the *Server Selection* page and click Next
- Deselect *FTP Server* under *Web Server (IIS)* on the *Roles* page
- Click Next and *Remove* as prompted (if installed).

Default Value:

Not Installed (Automatic when installed)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224851
Rule ID: SV-224851r569186_rule
STIG ID: WN16-00-000360
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

5.2 Ensure 'Peer Name Resolution Protocol (PNRPsvc)' is set to 'Not Installed' (STIG only) (Automated)

Profile Applicability:

- STIG Member Server
- STIG Domain Controller

Description:

This policy setting enables serverless peer name resolution over the Internet using the Peer Name Resolution Protocol (PNRP).

The STIG recommended state for this setting is: **Not Installed**.

Rationale:

Peer Name Resolution Protocol is a distributed and (mostly) serverless way to handle name resolution of clients with each other. In a high security environment, it is more secure to rely on centralized name resolution methods maintained by authorized staff.

Impact:

Some peer-to-peer and collaborative applications, such as Remote Assistance, may not function.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location and when set properly a **REG_DWORD** value **does not exist**.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PNRPsvc:Start

Note: Alternately this Windows Feature can be uninstalled by using *Roles and Features* in Server Manager.

Remediation:

To establish the recommended configuration via GP, set the following UI path to: **Not Installed**.

Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Peer Name Resolution Protocol

OR

To Uninstall the *Peer Name Resolution Protocol* feature:

- Start "Server Manager"
- Select the server with the role
- Scroll down to "ROLES AND FEATURES" in the right pane
- Select "Remove Roles and Features" from the drop-down "TASKS" list
- Select the appropriate server on the "Server Selection" page and click "Next"
- Deselect "Peer Name Resolution Protocol" on the "Features" page
- Click "Next" and "Remove" as prompted (if installed).

Default Value:

Manual

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224852
Rule ID: SV-224852r569186_rule
STIG ID: WN16-00-000370
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

5.3 Ensure 'Print Spooler (Spooler)' is set to 'Disabled' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This service spools print jobs and handles interaction with printers.

The recommended state for this setting is: **Disabled**.

Rationale:

Disabling the Print Spooler (Spooler) service mitigates the PrintNightmare vulnerability ([CVE-2021-34527](#)) and other attacks against the service.

Impact:

Domain Controllers will not be able to prune published printers from Active Directory. By default, Domain Controllers prune printer objects from Active Directory if the computer that published them doesn't respond to contact requests.

Domain Controllers will not be able to act as a print server, sharing printers for clients.

Applications on and users logged in at Domain Controllers will not be able to print, including printing to files (such as Adobe Portable Document Format (PDF)) which uses the Print Spooler service.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **4**.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Spooler:Start
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to: **Disabled**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Print Spooler
```

Default Value:

Automatic

References:

1. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

5.4 Ensure 'Print Spooler (Spooler)' is set to 'Disabled' (MS only) (Automated)

Profile Applicability:

- Level 2 - Member Server

Description:

This service spools print jobs and handles interaction with printers.

The recommended state for this setting is: **Disabled**.

Rationale:

Disabling the Print Spooler (Spooler) service mitigates the PrintNightmare vulnerability ([CVE-2021-34527](https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527)) and other attacks against the service.

Impact:

Member Servers will not be able to act as a print server, sharing printers for clients.

Applications on and users logged in to Member Servers will not be able to print, including printing to files (such as Adobe Portable Document Format (PDF)) which uses the Print Spooler service.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **4**.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Spooler:Start
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to: **Disabled**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Print Spooler
```

Default Value:

Automatic

References:

1. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

5.5 Ensure 'Simple TCP/IP Services (simptcp)' is set to 'Not Installed' (Automated)

Profile Applicability:

- STIG Member Server
- STIG Domain Controller

Description:

This policy setting supports the following TCP/IP services: Character Generator, Daytime, Discard, Echo, and Quote of the Day.

The STIG recommended state for this setting is: **Not Installed**.

Note: This service is not installed by default. It is supplied with Windows, but is installed by enabling an optional Windows feature (*Simple TCPIP services (i.e. echo, daytime etc)*).

Rationale:

The Simple TCP/IP Services have very little purpose in a modern enterprise environment - allowing them might increase exposure and risk for attack.

Impact:

The Simple TCP/IP services (Character Generator, Daytime, Discard, Echo and Quote of the Day) will not be available.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\simptcp:Start

Note: Alternately this Windows Feature can be uninstalled by using *Roles and Features* in Server Manager.

Remediation:

To establish the recommended configuration via GP, set the following UI path to: **Disabled** or ensure the service is not installed.

```
Computer Configuration\Policies\Windows Settings\Security Settings\System
Services\Simple TCP/IP Services
```

OR

To Uninstall the *Simple TCP/IP Services (simptcp)* feature:

- Start "Server Manager"
- Select the server with the role
- Scroll down to "ROLES AND FEATURES" in the right pane
- Select "Remove Roles and Features" from the drop-down "TASKS" list
- Select the appropriate server on the "Server Selection" page and click "Next"
- Deselect "Simple TCP/IP Services" on the "Features" page
- Click "Next" and "Remove" as prompted (if installed).

Default Value:

Not Installed (Automatic when installed)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224853
Rule ID: SV-224853r569186_rule
STIG ID: WN16-00-000380
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

6 Registry

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

7 File System

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

8 Wired Network (IEEE 802.3) Policies

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

9 Windows Defender Firewall with Advanced Security (formerly Windows Firewall with Advanced Security)

This section contains recommendations for configuring the Windows Firewall.

Note: In older versions of Microsoft Windows, this section was named *Windows Firewall with Advanced Security*, but it was renamed to *Windows Defender Firewall with Advanced Security* starting with the Server 2019 release.

9.1 Domain Profile

This section contains recommendations for the Domain Profile of the Windows Firewall.

9.1.1 Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

Select On (recommended) to have Windows Firewall with Advanced Security use the settings for this profile to filter network traffic. If you select Off, Windows Firewall with Advanced Security will not use any of the firewall rules or connection security rules for this profile.

The recommended state for this setting is: **On (recommended)**.

Rationale:

If the firewall is turned off all traffic will be able to access the system and an attacker may be more easily able to remotely exploit a weakness in a network service.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile:EnableFirewall

Remediation:

To establish the recommended configuration via GP, set the following UI path to **On (recommended)**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Defender Firewall with Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender Firewall Properties\Domain Profile\Firewall state
```

Default Value:

On (recommended). (The Windows Firewall with Advanced Security will be active in this profile.)

Additional Information:

Microsoft Windows Defender Firewall with Advanced Security Security Technical Implementation Guide:

Version 2, Release 2, Benchmark Date: November 09, 2023

Vul ID: V-241989

Rule ID: SV-241989r922928_rule

STIG ID: WNFWA-000001

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 <u>Implement and Manage a Firewall on End-User Devices</u> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			

9.1.2 Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This setting determines the behavior for inbound connections that do not match an inbound firewall rule.

The recommended state for this setting is: **Block (default)**.

Rationale:

If the firewall allows all traffic to access the system then an attacker may be more easily able to remotely exploit a weakness in a network service.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile:DefaultInboundAction
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Block (default)**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Defender Firewall with Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender Firewall Properties\Domain Profile\Inbound connections
```

Default Value:

Block (default). (The Windows Firewall with Advanced Security will block all inbound connections that do not match an inbound firewall rule in this profile.)

Additional Information:

Microsoft Windows Defender Firewall with Advanced Security Security Technical Implementation Guide:

Version 2, Release 2, Benchmark Date: November 09, 2023

Vul ID: V-241992

Rule ID: SV-241992r922934_rule

STIG ID: WNFWA-000004

Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 <u>Implement and Manage a Firewall on End-User Devices</u> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	11.2 <u>Document Traffic Configuration Rules</u> All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.			

9.1.3 Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)' (STIG only) (Automated)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This setting determines the behavior for outbound connections that do not match an outbound firewall rule.

The recommended state for this setting is: **Allow (default)**.

Rationale:

Some people believe that it is prudent to block all outbound connections except those specifically approved by the user or administrator. Microsoft disagrees with this opinion, blocking outbound connections by default will force users to deal with a large number of dialog boxes prompting them to authorize or block applications such as their web browser or instant messaging software. Additionally, blocking outbound traffic has little value because if an attacker has compromised the system they can reconfigure the firewall anyway.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile: DefaultOutboundAction

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Allow (default)**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Outbound connections
```

Default Value:

Allow (default). (The Windows Firewall with Advanced Security will allow all outbound connections in this profile unless there is a firewall rule explicitly blocking it.)

Additional Information:

Microsoft Windows Defender Firewall with Advanced Security Security Technical Implementation Guide:
Version 2, Release 2, Benchmark Date: November 09, 2023

Vul ID: V-241993
Rule ID: SV-241993r922936_rule
STIG ID: WNFWA-000005
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 <u>Implement and Manage a Firewall on End-User Devices</u> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	11.2 <u>Document Traffic Configuration Rules</u> All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.			

9.1.4 Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Select this option to have Windows Firewall with Advanced Security display notifications to the user when a program is blocked from receiving inbound connections.

The recommended state for this setting is: **No**.

Note: When the **Apply local firewall rules** setting is configured to **No**, it's recommended to also configure the **Display a notification setting** to **No**. Otherwise, users will continue to receive messages that ask if they want to unblock a restricted inbound connection, but the user's response will be ignored.

Rationale:

Firewall notifications can be complex and may confuse the end users, who would not be able to address the alert.

Impact:

Windows Firewall will not display a notification when a program is blocked from receiving inbound connections.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile:DisableNotifications
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **No**:

Computer Configuration\Policies\Windows Settings\Security Settings\Windows Defender Firewall with Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender Firewall Properties\Domain Profile\Settings Customize\Display a notification

Default Value:

Yes. (Windows Firewall with Advanced Security will display a notification when a program is blocked from receiving inbound connections.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 <u>Implement and Manage a Firewall on End-User Devices</u> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	11.2 <u>Document Traffic Configuration Rules</u> All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.			

9.1.5 Ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\domainfw.log' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

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.

Impact:

The log file will be stored in the specified file.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_SZ` value of `%SystemRoot%\System32\logfiles\firewall\domainfw.log`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\
Logging:LogFilePath
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to
%SystemRoot%\System32\logfiles\firewall\domainfw.log:

Computer Configuration\Policies\Windows Settings\Security Settings\Windows Defender Firewall with Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender Firewall Properties\Domain Profile\Logging Customize\Name

Default Value:

%SystemRoot%\System32\logfiles\firewall\pfirewall.log

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 <u>Implement and Manage a Firewall on End-User Devices</u> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	11.2 <u>Document Traffic Configuration Rules</u> All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.			

9.1.6 Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

Use this option to specify the size limit of the file in which Windows Firewall will write its log information.

The recommended state for this setting is: **16,384 KB or greater**.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Impact:

The log file size will be limited to the specified size, old events will be overwritten by newer ones when the limit is reached.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **16384**.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\Logging\LogFileSize
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **16,384 KB or greater**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Defender Firewall with Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender Firewall Properties\Domain Profile\Logging Customize\Size limit (KB)
```

Default Value:

4,096 KB.

Additional Information:

Microsoft Windows Defender Firewall with Advanced Security Security Technical Implementation Guide:

Version 2, Release 2, Benchmark Date: November 09, 2023

Vul ID: V-241994

Rule ID: SV-241994r922938_rule

STIG ID: WNFWA-000009

Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 <u>Implement and Manage a Firewall on End-User Devices</u> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	11.2 <u>Document Traffic Configuration Rules</u> All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.			

9.1.7 Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

Use this option to log when Windows Firewall with Advanced Security discards an inbound packet for any reason. The log records why and when the packet was dropped. Look for entries with the word **DROP** in the action column of the log.

The recommended state for this setting is: **Yes**.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Impact:

Information about dropped packets will be recorded in the firewall log file.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\Logging\LogDroppedPackets
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Yes**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Defender Firewall with Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender Firewall Properties\Domain Profile\Logging Customize\Log dropped packets
```

Default Value:

No (default). (Information about dropped packets will not be recorded in the firewall log file.)

Additional Information:

Microsoft Windows Defender Firewall with Advanced Security Security Technical Implementation Guide:

Version 2, Release 2, Benchmark Date: November 09, 2023

Vul ID: V-241995

Rule ID: SV-241995r922940_rule

STIG ID: WNFWA-000010

Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 <u>Implement and Manage a Firewall on End-User Devices</u> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	11.2 <u>Document Traffic Configuration Rules</u> All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.			

9.1.8 Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

Use this option to log when Windows Firewall with Advanced Security allows an inbound connection. The log records why and when the connection was formed. Look for entries with the word **ALLOW** in the action column of the log.

The recommended state for this setting is: **Yes**.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Impact:

Information about successful connections will be recorded in the firewall log file.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\Logging\LogSuccessfulConnections
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Yes**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Defender Firewall with Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender Firewall Properties\Domain Profile\Logging Customize\Log successful connections
```

Default Value:

No (default). (Information about successful connections will not be recorded in the firewall log file.)

Additional Information:

Microsoft Windows Defender Firewall with Advanced Security Security Technical Implementation Guide:

Version 2, Release 2, Benchmark Date: November 09, 2023

Vul ID: V-241996

Rule ID: SV-241996r922942_rule

STIG ID: WNFWA-000011

Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 <u>Implement and Manage a Firewall on End-User Devices</u> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	11.2 <u>Document Traffic Configuration Rules</u> All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.			

9.2 Private Profile

This section contains recommendations for the Private Profile of the Windows Firewall.

9.2.1 Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

Select On (recommended) to have Windows Firewall with Advanced Security use the settings for this profile to filter network traffic. If you select Off, Windows Firewall with Advanced Security will not use any of the firewall rules or connection security rules for this profile.

The recommended state for this setting is: **On (recommended)**.

Rationale:

If the firewall is turned off all traffic will be able to access the system and an attacker may be more easily able to remotely exploit a weakness in a network service.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile:EnableFirewal  
1
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **On (recommended)**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Defender Firewall with Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender Firewall Properties\Private Profile\Firewall state
```

Default Value:

On (recommended). (The Windows Firewall with Advanced Security will be active in this profile.)

Additional Information:

Microsoft Windows Defender Firewall with Advanced Security Security Technical Implementation Guide:

Version 2, Release 2, Benchmark Date: November 09, 2023

Vul ID: V-241990

Rule ID: SV-241990r922930_rule

STIG ID: WNFWA-000002

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 <u>Implement and Manage a Firewall on End-User Devices</u> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			

9.2.2 Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This setting determines the behavior for inbound connections that do not match an inbound firewall rule.

The recommended state for this setting is: **Block (default)**.

Rationale:

If the firewall allows all traffic to access the system then an attacker may be more easily able to remotely exploit a weakness in a network service.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile:DefaultInboundAction
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Block (default)**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Defender Firewall with Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender Firewall Properties\Private Profile\Inbound connections
```

Default Value:

Block (default). (The Windows Firewall with Advanced Security will block all inbound connections that do not match an inbound firewall rule in this profile.)

Additional Information:

Microsoft Windows Defender Firewall with Advanced Security Security Technical Implementation Guide:

Version 2, Release 2, Benchmark Date: November 09, 2023

Vul ID: V-241997

Rule ID: SV-241997r922944_rule

STIG ID: WNFWA-000012

Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 <u>Implement and Manage a Firewall on End-User Devices</u> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	11.2 <u>Document Traffic Configuration Rules</u> All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.			

9.2.3 Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)' (STIG only) (Automated)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This setting determines the behavior for outbound connections that do not match an outbound firewall rule.

The recommended state for this setting is: **Allow (default)**.

Note: If you set Outbound connections to Block and then deploy the firewall policy by using a GPO, computers that receive the GPO settings cannot receive subsequent Group Policy updates unless you create and deploy an outbound rule that enables Group Policy to work. Predefined rules for Core Networking include outbound rules that enable Group Policy to work. Ensure that these outbound rules are active, and thoroughly test firewall profiles before deploying.

Rationale:

Some people believe that it is prudent to block all outbound connections except those specifically approved by the user or administrator. Microsoft disagrees with this opinion, blocking outbound connections by default will force users to deal with a large number of dialog boxes prompting them to authorize or block applications such as their web browser or instant messaging software. Additionally, blocking outbound traffic has little value because if an attacker has compromised the system they can reconfigure the firewall anyway.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile  
:DefaultOutboundAction
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Allow (default)**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Outbound connections
```

Default Value:

Allow (default). (The Windows Firewall with Advanced Security will allow all outbound connections in this profile unless there is a firewall rule explicitly blocking it.)

Additional Information:

```
Microsoft Windows Defender Firewall with Advanced Security Security Technical Implementation Guide:  
Version 2, Release 2, Benchmark Date: November 09, 2023  
  
Vul ID: V-241998  
Rule ID: SV-241998r922946_rule  
STIG ID: WNFWA-000013  
Severity: CAT II
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 <u>Implement and Manage a Firewall on End-User Devices</u> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	11.2 <u>Document Traffic Configuration Rules</u> All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.			

9.2.4 Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Select this option to have Windows Firewall with Advanced Security display notifications to the user when a program is blocked from receiving inbound connections.

The recommended state for this setting is: **No**.

Note: When the **Apply local firewall rules** setting is configured to **No**, it's recommended to also configure the **Display a notification** setting to **No**. Otherwise, users will continue to receive messages that ask if they want to unblock a restricted inbound connection, but the user's response will be ignored.

Rationale:

Firewall notifications can be complex and may confuse the end users, who would not be able to address the alert.

Impact:

Windows Firewall will not display a notification when a program is blocked from receiving inbound connections.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile:DisableNotifications
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **No**:

Computer Configuration\Policies\Windows Settings\Security Settings\Windows Defender Firewall with Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender Firewall Properties\Private Profile\Settings Customize\Display a notification

Default Value:

Yes. (Windows Firewall with Advanced Security will display a notification when a program is blocked from receiving inbound connections.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 <u>Implement and Manage a Firewall on End-User Devices</u> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	11.2 <u>Document Traffic Configuration Rules</u> All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.			

9.2.5 Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\privatefw.log' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

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.

Impact:

The log file will be stored in the specified file.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_SZ` value of `%SystemRoot%\System32\logfiles\firewall\privatefw.log`.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile \Logging:LogFilePath

Remediation:

To establish the recommended configuration via GP, set the following UI path to
%SystemRoot%\System32\logfiles\firewall\privatefw.log:

Computer Configuration\Policies\Windows Settings\Security Settings\Windows Defender Firewall with Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender Firewall Properties\Private Profile\Logging Customize\Name

Default Value:

%SystemRoot%\System32\logfiles\firewall\pfirewall.log

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 <u>Implement and Manage a Firewall on End-User Devices</u> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	11.2 <u>Document Traffic Configuration Rules</u> All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.			

9.2.6 Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

Use this option to specify the size limit of the file in which Windows Firewall will write its log information.

The recommended state for this setting is: **16,384 KB or greater**.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Impact:

The log file size will be limited to the specified size, old events will be overwritten by newer ones when the limit is reached.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **16384**.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile\Logging\LogFileSize
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **16,384 KB or greater**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Defender Firewall with Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender Firewall Properties\Private Profile\Logging Customize\Size limit (KB)
```

Default Value:

4,096 KB.

Additional Information:

Microsoft Windows Defender Firewall with Advanced Security Security Technical Implementation Guide:

Version 2, Release 2, Benchmark Date: November 09, 2023

Vul ID: V-241999

Rule ID: SV-241999r922948_rule

STIG ID: WNFWA-000017

Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 <u>Implement and Manage a Firewall on End-User Devices</u> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	11.2 <u>Document Traffic Configuration Rules</u> All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.			

9.2.7 Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

Use this option to log when Windows Firewall with Advanced Security discards an inbound packet for any reason. The log records why and when the packet was dropped. Look for entries with the word **DROP** in the action column of the log.

The recommended state for this setting is: **Yes**.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Impact:

Information about dropped packets will be recorded in the firewall log file.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile\Logging\LogDroppedPackets
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Yes**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Defender Firewall with Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender Firewall Properties\Private Profile\Logging Customize\Log dropped packets
```

Default Value:

No (default). (Information about dropped packets will not be recorded in the firewall log file.)

Additional Information:

Microsoft Windows Defender Firewall with Advanced Security Security Technical Implementation Guide:

Version 2, Release 2, Benchmark Date: November 09, 2023

Vul ID: V-242000

Rule ID: SV-242000r922950_rule

STIG ID: WNFWA-000018

Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 <u>Implement and Manage a Firewall on End-User Devices</u> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	11.2 <u>Document Traffic Configuration Rules</u> All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.			

9.2.8 Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

Use this option to log when Windows Firewall with Advanced Security allows an inbound connection. The log records why and when the connection was formed. Look for entries with the word **ALLOW** in the action column of the log.

The recommended state for this setting is: **Yes**.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Impact:

Information about successful connections will be recorded in the firewall log file.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile\Logging\LogSuccessfulConnections
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Yes**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Defender Firewall with Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender Firewall Properties\Private Profile\Logging Customize\Log successful connections
```

Default Value:

No (default). (Information about successful connections will not be recorded in the firewall log file.)

Additional Information:

Microsoft Windows Defender Firewall with Advanced Security Security Technical Implementation Guide:

Version 2, Release 2, Benchmark Date: November 09, 2023

Vul ID: V-242001

Rule ID: SV-242001r922952_rule

STIG ID: WNFWA-000019

Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 <u>Implement and Manage a Firewall on End-User Devices</u> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	11.2 <u>Document Traffic Configuration Rules</u> All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.			

9.3 Public Profile

This section contains recommendations for the Public Profile of the Windows Firewall.

9.3.1 Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

Select On (recommended) to have Windows Firewall with Advanced Security use the settings for this profile to filter network traffic. If you select Off, Windows Firewall with Advanced Security will not use any of the firewall rules or connection security rules for this profile.

The recommended state for this setting is: **On (recommended)**.

Rationale:

If the firewall is turned off all traffic will be able to access the system and an attacker may be more easily able to remotely exploit a weakness in a network service.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile:EnableFirewall

Remediation:

To establish the recommended configuration via GP, set the following UI path to **On (recommended)**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Defender Firewall with Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender Firewall Properties\Public Profile\Firewall state
```

Default Value:

On (recommended). (The Windows Firewall with Advanced Security will be active in this profile.)

Additional Information:

Microsoft Windows Defender Firewall with Advanced Security Security Technical Implementation Guide:

Version 2, Release 2, Benchmark Date: November 09, 2023

Vul ID: V-241991

Rule ID: SV-241991r922932_rule

STIG ID: WNFWA-000003

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			

9.3.2 Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This setting determines the behavior for inbound connections that do not match an inbound firewall rule.

The recommended state for this setting is: **Block (default)**.

Rationale:

If the firewall allows all traffic to access the system then an attacker may be more easily able to remotely exploit a weakness in a network service.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile:DefaultInboundAction
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Block (default)**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Defender Firewall with Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender Firewall Properties\Public Profile\Inbound connections
```

Default Value:

Block (default). (The Windows Firewall with Advanced Security will block all inbound connections that do not match an inbound firewall rule in this profile.)

Additional Information:

Microsoft Windows Defender Firewall with Advanced Security Security Technical Implementation Guide:

Version 2, Release 2, Benchmark Date: November 09, 2023

Vul ID: V-242002

Rule ID: SV-242002r922954_rule

STIG ID: WNFWA-000020

Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 <u>Implement and Manage a Firewall on End-User Devices</u> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	11.2 <u>Document Traffic Configuration Rules</u> All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.			

9.3.3 Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)' (STIG only) (Automated)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This setting determines the behavior for outbound connections that do not match an outbound firewall rule.

The recommended state for this setting is: **Allow (default)**.

Note: If you set Outbound connections to Block and then deploy the firewall policy by using a GPO, computers that receive the GPO settings cannot receive subsequent Group Policy updates unless you create and deploy an outbound rule that enables Group Policy to work. Predefined rules for Core Networking include outbound rules that enable Group Policy to work. Ensure that these outbound rules are active, and thoroughly test firewall profiles before deploying.

Rationale:

Some people believe that it is prudent to block all outbound connections except those specifically approved by the user or administrator. Microsoft disagrees with this opinion, blocking outbound connections by default will force users to deal with a large number of dialog boxes prompting them to authorize or block applications such as their web browser or instant messaging software. Additionally, blocking outbound traffic has little value because if an attacker has compromised the system they can reconfigure the firewall anyway.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile:
DefaultOutboundAction
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Allow (default)**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Outbound connections
```

Default Value:

Allow (default). (The Windows Firewall with Advanced Security will allow all outbound connections in this profile unless there is a firewall rule explicitly blocking it.)

Additional Information:

```
Microsoft Windows Defender Firewall with Advanced Security Security Technical Implementation Guide:  
Version 2, Release 2, Benchmark Date: November 09, 2023  
  
Vul ID: V-242003  
Rule ID: SV-242003r922956_rule  
STIG ID: WNFWA-000021  
Severity: CAT II
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 <u>Implement and Manage a Firewall on End-User Devices</u> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	11.2 <u>Document Traffic Configuration Rules</u> All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.			

9.3.4 Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'No' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Select this option to have Windows Firewall with Advanced Security display notifications to the user when a program is blocked from receiving inbound connections.

The recommended state for this setting is: **No**.

Rationale:

Some organizations may prefer to avoid alarming users when firewall rules block certain types of network activity. However, notifications can be helpful when troubleshooting network issues involving the firewall.

Impact:

Windows Firewall will not display a notification when a program is blocked from receiving inbound connections.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile:DisableNotifications
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to 'No':

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Defender Firewall with Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender Firewall Properties\Public Profile\Settings Customize\Display a notification
```

Default Value:

Yes. (Windows Firewall with Advanced Security will display a notification when a program is blocked from receiving inbound connections.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 <u>Implement and Manage a Firewall on End-User Devices</u> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	11.2 <u>Document Traffic Configuration Rules</u> All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.			

9.3.5 Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This setting controls whether local administrators are allowed to create local firewall rules that apply together with firewall rules configured by Group Policy.

The recommended state for this setting is: **No**.

Note: When the **Apply local firewall rules** setting is configured to **No**, it's recommended to also configure the **Display a notification** setting to **No**. Otherwise, users will continue to receive messages that ask if they want to unblock a restricted inbound connection, but the user's response will be ignored.

Rationale:

When in the Public profile, there should be no special local firewall exceptions per computer. These settings should be managed by a centralized policy.

Impact:

Administrators can still create firewall rules, but the rules will not be applied.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile:AllowLocalPolicyMerge
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **No**:

Computer Configuration\Policies\Windows Settings\Security Settings\Windows Defender Firewall with Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender Firewall Properties\Public Profile\Settings Customize\Apply local firewall rules

Default Value:

Yes (default). (Firewall rules created by administrators will be applied.)

Additional Information:

Microsoft Windows Defender Firewall with Advanced Security Security Technical Implementation Guide:
Version 2, Release 2, Benchmark Date: November 09, 2023

Vul ID: V-242004
Rule ID: SV-242004r922958_rule
STIG ID: WNFWA-000024
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 <u>Implement and Manage a Firewall on End-User Devices</u> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	11.2 <u>Document Traffic Configuration Rules</u> All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.			

9.3.6 Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This setting controls whether local administrators are allowed to create connection security rules that apply together with connection security rules configured by Group Policy.

The recommended state for this setting is: **No**.

Rationale:

Users with administrative privileges might create firewall rules that expose the system to remote attack.

Impact:

Administrators can still create local connection security rules, but the rules will not be applied.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile:AllowLocalIPsecPolicyMerge
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **No**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Defender Firewall with Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender Firewall Properties\Public Profile\Settings Customize\Apply local connection security rules
```

Default Value:

Yes (default). (Local connection security rules created by administrators will be applied.)

Additional Information:

Microsoft Windows Defender Firewall with Advanced Security Security Technical Implementation Guide:

Version 2, Release 2, Benchmark Date: November 09, 2023

Vul ID: V-242005

Rule ID: SV-242005r922960_rule

STIG ID: WNFWA-000025

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 <u>Implement and Manage a Firewall on End-User Devices</u> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	11.2 <u>Document Traffic Configuration Rules</u> All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.			

9.3.7 Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\publicfw.log' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

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.

Impact:

The log file will be stored in the specified file.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_SZ` value of `%SystemRoot%\System32\logfiles\firewall\publicfw.log`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile\
Logging:LogFilePath
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to
%SystemRoot%\System32\logfiles\firewall\publicfw.log:

Computer Configuration\Policies\Windows Settings\Security Settings\Windows Defender Firewall with Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender Firewall Properties\Public Profile\Logging Customize\Name

Default Value:

%SystemRoot%\System32\logfiles\firewall\pfirewall.log

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 <u>Implement and Manage a Firewall on End-User Devices</u> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	11.2 <u>Document Traffic Configuration Rules</u> All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.			

9.3.8 Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

Use this option to specify the size limit of the file in which Windows Firewall will write its log information.

The recommended state for this setting is: **16,384 KB or greater**.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Impact:

The log file size will be limited to the specified size, old events will be overwritten by newer ones when the limit is reached.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **16384**.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile\Logging\LogFileSize
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **16,384 KB or greater**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Defender Firewall with Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender Firewall Properties\Public Profile\Logging Customize\Size limit (KB)
```

Default Value:

4,096 KB.

Additional Information:

Microsoft Windows Defender Firewall with Advanced Security Security Technical Implementation Guide:

Version 2, Release 2, Benchmark Date: November 09, 2023

Vul ID: V-242006

Rule ID: SV-242006r922962_rule

STIG ID: WNFWA-000027

Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 <u>Implement and Manage a Firewall on End-User Devices</u> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	11.2 <u>Document Traffic Configuration Rules</u> All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.			

9.3.9 Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

Use this option to log when Windows Firewall with Advanced Security discards an inbound packet for any reason. The log records why and when the packet was dropped. Look for entries with the word **DROP** in the action column of the log.

The recommended state for this setting is: **Yes**.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Impact:

Information about dropped packets will be recorded in the firewall log file.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile\Logging\LogDroppedPackets
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Yes**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Defender Firewall with Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender Firewall Properties\Public Profile\Logging Customize\Log dropped packets
```

Default Value:

No (default). (Information about dropped packets will not be recorded in the firewall log file.)

Additional Information:

Microsoft Windows Defender Firewall with Advanced Security Security Technical Implementation Guide:

Version 2, Release 2, Benchmark Date: November 09, 2023

Vul ID: V-242007

Rule ID: SV-242007r922964_rule

STIG ID: WNFWA-000028

Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 <u>Implement and Manage a Firewall on End-User Devices</u> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	11.2 <u>Document Traffic Configuration Rules</u> All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.			

9.3.10 Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Use this option to log when Windows Firewall with Advanced Security allows an inbound connection. The log records why and when the connection was formed. Look for entries with the word **ALLOW** in the action column of the log.

The recommended state for this setting is: **Yes**.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Impact:

Information about successful connections will be recorded in the firewall log file.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile\Logging\LogSuccessfulConnections
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Yes**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Defender Firewall with Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender Firewall Properties\Public Profile\Logging Customize\Log successful connections
```

Default Value:

No (default). (Information about successful connections will not be recorded in the firewall log file.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 <u>Implement and Manage a Firewall on End-User Devices</u> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	11.2 <u>Document Traffic Configuration Rules</u> All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.			

10 Network List Manager Policies

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

11 Wireless Network (IEEE 802.11) Policies

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

12 Public Key Policies

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

13 Software Restriction Policies

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

14 Network Access Protection NAP Client Configuration

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

15 Application Control Policies

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

16 IP Security Policies

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

17 Advanced Audit Policy Configuration

This section contains recommendations for configuring the Windows audit facilities.

17.1 Account Logon

This section contains recommendations for configuring the Account Logon audit policy.

17.1.1 Ensure 'Audit Credential Validation' is set to 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This subcategory reports the results of validation tests on credentials submitted for a user account logon request. These events occur on the computer that is authoritative for the credentials. For domain accounts, the Domain Controller is authoritative, whereas for local accounts, the local computer is authoritative. In domain environments, most of the Account Logon events occur in the Security log of the Domain Controllers that are authoritative for the domain accounts. However, these events can occur on other computers in the organization when local accounts are used to log on. Events for this subcategory include:

- 4774: An account was mapped for logon.
- 4775: An account could not be mapped for logon.
- 4776: The Domain Controller attempted to validate the credentials for an account.
- 4777: The Domain Controller failed to validate the credentials for an account.

The recommended state for this setting is: **Success and Failure**.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using **auditpol.exe**, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce923f-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Success and Failure**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Logon\Audit Credential Validation
```

Default Value:

Success.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224881 and V-224882
Rule ID: SV-224881r569186_rule and SV-224882r569186_rule
STIG ID: WN16-AU-000070 and WN16-AU-000080
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●
v7	16.12 Monitor Attempts to Access Deactivated Accounts Monitor attempts to access deactivated accounts through audit logging.		●	●

17.1.2 Ensure 'Audit Kerberos Authentication Service' is set to 'Success and Failure' (DC Only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This subcategory reports the results of events generated after a Kerberos authentication TGT request. Kerberos is a distributed authentication service that allows a client running on behalf of a user to prove its identity to a server without sending data across the network. This helps mitigate an attacker or server from impersonating a user.

- 4768: A Kerberos authentication ticket (TGT) was requested.
- 4771: Kerberos pre-authentication failed.
- 4772: A Kerberos authentication ticket request failed.

The recommended state for this setting is: **Success and Failure**.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using **auditpol.exe**, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9242-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Success and Failure**:

Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Logon\Audit Kerberos Authentication Service

Default Value:

Success.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

17.1.3 Ensure 'Audit Kerberos Service Ticket Operations' is set to 'Success and Failure' (DC Only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This subcategory reports the results of events generated by Kerberos authentication ticket-granting ticket (TGT) requests. Kerberos Service Ticket requests (TGS requests) occur as part of service use and access requests by specific accounts. Auditing these events will record the IP address from which the account requested TGS, when TGS was requested, and which encryption type was used.

- 4769: A Kerberos service ticket was requested.
- 4770: A Kerberos service ticket was renewed.
- 4773: A Kerberos service ticket request failed.

The recommended state for this setting is: **Success and Failure**.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using **auditpol.exe**, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9240-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Success and Failure**:

Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Logon\Audit Kerberos Service Ticket Operations

Default Value:

Success.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

17.2 Account Management

This section contains recommendations for configuring the Account Management audit policy.

17.2.1 Ensure 'Audit Application Group Management' is set to 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to audit events generated by changes to application groups such as the following:

- Application group is created, changed, or deleted.
- Member is added or removed from an application group.

Application groups are utilized by Windows Authorization Manager, which is a flexible framework created by Microsoft for integrating role-based access control (RBAC) into applications. More information on Windows Authorization Manager is available at [MSDN - Windows Authorization Manager](#).

The recommended state for this setting is: **Success and Failure**.

Note: Although Microsoft "[Deprecated](#)" Windows Authorization Manager (AzMan) in Windows Server 2012 and 2012 R2, this feature still exists in the OS (unimproved), and therefore should still be audited.

Rationale:

Auditing events in this category may be useful when investigating an incident.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using **auditpol.exe**, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9239-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Success and Failure**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Application Group Management
```

Default Value:

No Auditing.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

17.2.2 Ensure 'Audit Computer Account Management' is set to include 'Success' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- STIG Domain Controller

Description:

This subcategory reports each event of computer account management, such as when a computer account is created, changed, deleted, renamed, disabled, or enabled. Events for this subcategory include:

- 4741: A computer account was created.
- 4742: A computer account was changed.
- 4743: A computer account was deleted.

The recommended state for this setting is to include: **Success**.

Rationale:

Auditing events in this category may be useful when investigating an incident.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using **auditpol.exe**, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9236-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to include **Success**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Computer Account Management
```

Default Value:

Success.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224986
Rule ID: SV-224986r852358_rule
STIG ID: WN16-DC-000230
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

17.2.3 Ensure 'Audit Distribution Group Management' is set to include 'Success' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This subcategory reports each event of distribution group management, such as when a distribution group is created, changed, or deleted or when a member is added to or removed from a distribution group. If you enable this Audit policy setting, administrators can track events to detect malicious, accidental, and authorized creation of group accounts. Events for this subcategory include:

- 4744: A security-disabled local group was created.
- 4745: A security-disabled local group was changed.
- 4746: A member was added to a security-disabled local group.
- 4747: A member was removed from a security-disabled local group.
- 4748: A security-disabled local group was deleted.
- 4749: A security-disabled global group was created.
- 4750: A security-disabled global group was changed.
- 4751: A member was added to a security-disabled global group.
- 4752: A member was removed from a security-disabled global group.
- 4753: A security-disabled global group was deleted.
- 4759: A security-disabled universal group was created.
- 4760: A security-disabled universal group was changed.
- 4761: A member was added to a security-disabled universal group.
- 4762: A member was removed from a security-disabled universal group.
- 4763: A security-disabled universal group was deleted.

The recommended state for this setting is to include: **Success**.

Rationale:

Auditing these events may provide an organization with insight when investigating an incident. For example, when a given unauthorized user was added to a sensitive distribution group.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using **auditpol.exe**, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9238-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to include **Success**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Distribution Group Management
```

Default Value:

No Auditing.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

17.2.4 Ensure 'Audit Other Account Management Events' is set to include 'Success' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This subcategory reports other account management events. Events for this subcategory include:

- 4782: The password hash an account was accessed.
- 4793: The Password Policy Checking API was called.

The recommended state for this setting is to include: **Success**.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using **auditpol.exe**, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce923a-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to include **Success**:

Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Other Account Management Events

Default Value:

No Auditing.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

17.2.5 Ensure 'Audit Other Account Management Events' is set to include 'Success' (STIG Only) (Automated)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This subcategory reports other account management events. Events for this subcategory include:

- 4782: The password hash an account was accessed.
- 4793: The Password Policy Checking API was called.

The recommended STIG state for this setting is to include: **Success**.

Note: The CIS recommended state for this setting is: **Success** for Domain Controllers only, which differs from the STIG recommended state of Domain Controllers and Member Servers.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using **auditpol.exe**, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce923a-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to include **Success**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Other Account Management Events
```

Default Value:

No Auditing.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224883
Rule ID: SV-224883r852305_rule
STIG ID: WN16-AU-000100
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

17.2.6 Ensure 'Audit Security Group Management' is set to include 'Success' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This subcategory reports each event of security group management, such as when a security group is created, changed, or deleted or when a member is added to or removed from a security group. If you enable this Audit policy setting, administrators can track events to detect malicious, accidental, and authorized creation of security group accounts. Events for this subcategory include:

- 4727: A security-enabled global group was created.
- 4728: A member was added to a security-enabled global group.
- 4729: A member was removed from a security-enabled global group.
- 4730: A security-enabled global group was deleted.
- 4731: A security-enabled local group was created.
- 4732: A member was added to a security-enabled local group.
- 4733: A member was removed from a security-enabled local group.
- 4734: A security-enabled local group was deleted.
- 4735: A security-enabled local group was changed.
- 4737: A security-enabled global group was changed.
- 4754: A security-enabled universal group was created.
- 4755: A security-enabled universal group was changed.
- 4756: A member was added to a security-enabled universal group.
- 4757: A member was removed from a security-enabled universal group.
- 4758: A security-enabled universal group was deleted.
- 4764: A group's type was changed.

The recommended state for this setting is to include: **Success**.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using **auditpol.exe**, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9237-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to include **Success**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced  
Audit Policy Configuration\Audit Policies\Account Management\Audit Security  
Group Management
```

Default Value:

Success.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224884
Rule ID: SV-224884r852306_rule
STIG ID: WN16-AU-000120
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			
v7	16.6 <u>Maintain an Inventory of Accounts</u> Maintain an inventory of all accounts organized by authentication system.			

17.2.7 Ensure 'Audit User Account Management' is set to 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This subcategory reports each event of user account management, such as when a user account is created, changed, or deleted; a user account is renamed, disabled, or enabled; or a password is set or changed. If you enable this Audit policy setting, administrators can track events to detect malicious, accidental, and authorized creation of user accounts. Events for this subcategory include:

- 4720: A user account was created.
- 4722: A user account was enabled.
- 4723: An attempt was made to change an account's password.
- 4724: An attempt was made to reset an account's password.
- 4725: A user account was disabled.
- 4726: A user account was deleted.
- 4738: A user account was changed.
- 4740: A user account was locked out.
- 4765: SID History was added to an account.
- 4766: An attempt to add SID History to an account failed.
- 4767: A user account was unlocked.
- 4780: The ACL was set on accounts which are members of administrators groups.
- 4781: The name of an account was changed:
- 4794: An attempt was made to set the Directory Services Restore Mode.
- 5376: Credential Manager credentials were backed up.
- 5377: Credential Manager credentials were restored from a backup.

The recommended state for this setting is: **Success and Failure**.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using **auditpol.exe**, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9235-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to

Success and Failure:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced  
Audit Policy Configuration\Audit Policies\Account Management\Audit User  
Account Management
```

Default Value:

Success.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224885 and V-224886
Rule ID: SV-224885r852307_rule and SV-224886r852308_rule
STIG ID: WN16-AU-000140 and WN16-AU-000150
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

17.3 Detailed Tracking

This section contains recommendations for configuring the Detailed Tracking audit policy.

17.3.1 Ensure 'Audit PNP Activity' is set to include 'Success' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting allows you to audit when plug and play detects an external device.

The recommended state for this setting is to include: **Success**.

Note: A Windows 10, Server 2016 or newer OS is required to access and set this value in Group Policy.

Rationale:

Enabling this setting will allow a user to audit events when a device is plugged into a system. This can help alert IT staff if unapproved devices are plugged in.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using **auditpol.exe**, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9248-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to include **Success:**

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Detailed Tracking\Audit PNP Activity
```

Default Value:

No Auditing.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224887
Rule ID: SV-224887r569186_rule
STIG ID: WN16-AU-000160
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

17.3.2 Ensure 'Audit Process Creation' is set to include 'Success' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This subcategory reports the creation of a process and the name of the program or user that created it. Events for this subcategory include:

- 4688: A new process has been created.
- 4696: A primary token was assigned to process.

Refer to Microsoft Knowledge Base article 947226: [Description of security events in Windows Vista and in Windows Server 2008](#) for the most recent information about this setting.

The recommended state for this setting is to include: **Success**.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using **auditpol.exe**, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce922b-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to include **Success**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Detailed Tracking\Audit Process Creation
```

Default Value:

No Auditing.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224888
Rule ID: SV-224888r852309_rule
STIG ID: WN16-AU-000170
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

17.4 DS Access

This section contains recommendations for configuring the Directory Services Access audit policy.

17.4.1 Ensure 'Audit Directory Service Access' is set to include 'Failure' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This subcategory reports when an AD DS object is accessed. Only objects with SACLs cause audit events to be generated, and only when they are accessed in a manner that matches their SACL. These events are similar to the directory service access events in previous versions of Windows Server. This subcategory applies only to Domain Controllers. Events for this subcategory include:

- 4662: An operation was performed on an object.

The recommended state for this setting is to include: **Failure**.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using **auditpol.exe**, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce923b-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to include **Failure**:

Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\DS Access\Audit Directory Service Access

Default Value:

Success.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

17.4.2 Ensure 'Audit Directory Service Access' is set to include 'Success and Failure' (STIG DC only) (Automated)

Profile Applicability:

- STIG Domain Controller

Description:

This subcategory reports when an AD DS object is accessed. Only objects with SACLs cause audit events to be generated, and only when they are accessed in a manner that matches their SACL. These events are similar to the directory service access events in previous versions of Windows Server. This subcategory applies only to Domain Controllers. Events for this subcategory include:

- 4662 : An operation was performed on an object.

The recommended state for this setting is to include: **Success and Failure**.

Note: The CIS recommended state for this setting is: **Failure**, which differs from the STIG recommended state.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using **auditpol.exe**, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce923b-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to include **Success and Failure**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\DS Access\Audit Directory Service Access
```

Default Value:

Success.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224987 and V-224988
Rule ID: SV-224891r569186_rule and SV-224892r569186_rule
STIG ID: WN16-DC-000240 and WN16-DC-000250
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

17.4.3 Ensure 'Audit Directory Service Changes' is set to include 'Success' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- STIG Domain Controller

Description:

This subcategory reports changes to objects in Active Directory Domain Services (AD DS). The types of changes that are reported are create, modify, move, and undelete operations that are performed on an object. DS Change auditing, where appropriate, indicates the old and new values of the changed properties of the objects that were changed. Only objects with SACLs cause audit events to be generated, and only when they are accessed in a manner that matches their SACL. Some objects and properties do not cause audit events to be generated due to settings on the object class in the schema. This subcategory applies only to Domain Controllers. Events for this subcategory include:

- 5136: A directory service object was modified.
- 5137: A directory service object was created.
- 5138: A directory service object was undeleted.
- 5139: A directory service object was moved.

The recommended state for this setting is to include: **Success**.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using **auditpol.exe**, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce923c-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to include **Success**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\DS Access\Audit Directory Service Changes
```

Default Value:

No Auditing.

Additional Information:

```
Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID:      V-224989
Rule ID:     SV-224989r852361_rule
STIG ID:     WN16-DC-000260
Severity:    CAT II
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

17.5 Logon/Logoff

This section contains recommendations for configuring the Logon/Logoff audit policy.

17.5.1 Ensure 'Audit Account Lockout' is set to include 'Failure' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This subcategory reports when a user's account is locked out as a result of too many failed logon attempts. Events for this subcategory include:

- 4625: An account failed to log on.

The recommended state for this setting is to include: **Failure**.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using **auditpol.exe**, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9217-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to include **Failure**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Account Lockout
```

Default Value:

Success.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224889
Rule ID: SV-224889r569186_rule
STIG ID: WN16-AU-000220
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●
v7	16.6 Maintain an Inventory of Accounts Maintain an inventory of all accounts organized by authentication system.		●	●

17.5.2 Ensure 'Audit Group Membership' is set to include 'Success' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy allows you to audit the group membership information in the user's logon token. Events in this subcategory are generated on the computer on which a logon session is created. For an interactive logon, the security audit event is generated on the computer that the user logged on to. For a network logon, such as accessing a shared folder on the network, the security audit event is generated on the computer hosting the resource.

The recommended state for this setting is to include: **Success**.

Note: A Windows 10, Server 2016 or newer OS is required to access and set this value in Group Policy.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using **auditpol.exe**, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9249-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to include **Success**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Group Membership
```

Default Value:

No Auditing.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224891
Rule ID: SV-224891r569186_rule
STIG ID: WN16-AU-000240
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

17.5.3 Ensure 'Audit Logoff' is set to include 'Success' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This subcategory reports when a user logs off from the system. These events occur on the accessed computer. For interactive logons, the generation of these events occurs on the computer that is logged on to. If a network logon takes place to access a share, these events generate on the computer that hosts the accessed resource. If you configure this setting to No auditing, it is difficult or impossible to determine which user has accessed or attempted to access organization computers. Events for this subcategory include:

- 4634: An account was logged off.
- 4647: User initiated logoff.

The recommended state for this setting is to include: **Success**.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using **auditpol.exe**, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9216-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to include **Success**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Logoff
```

Default Value:

Success.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224892
Rule ID: SV-224892r569186_rule
STIG ID: WN16-AU-000250
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●
v7	16.13 Alert on Account Login Behavior Deviation Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

17.5.4 Ensure 'Audit Logon' is set to 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This subcategory reports when a user attempts to log on to the system. These events occur on the accessed computer. For interactive logons, the generation of these events occurs on the computer that is logged on to. If a network logon takes place to access a share, these events generate on the computer that hosts the accessed resource. If you configure this setting to No auditing, it is difficult or impossible to determine which user has accessed or attempted to access organization computers. Events for this subcategory include:

- 4624: An account was successfully logged on.
- 4625: An account failed to log on.
- 4648: A logon was attempted using explicit credentials.
- 4675: SIDs were filtered.

The recommended state for this setting is: **Success and Failure**.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using **auditpol.exe**, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9215-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Success and Failure**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Logon
```

Default Value:

Success and Failure.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide: Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224893 and V-224894 Rule ID: SV-224893r569186_rule and SV-224894r569186_rule STIG ID: WN16-AU-000260 and WN16-AU-000270 Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			
v7	16.13 <u>Alert on Account Login Behavior Deviation</u> Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			

17.5.5 Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports other logon/logoff-related events, such as Remote Desktop Services session disconnects and reconnects, using RunAs to run processes under a different account, and locking and unlocking a workstation. Events for this subcategory include:

- 4649: A replay attack was detected.
- 4778: A session was reconnected to a Window Station.
- 4779: A session was disconnected from a Window Station.
- 4800: The workstation was locked.
- 4801: The workstation was unlocked.
- 4802: The screen saver was invoked.
- 4803: The screen saver was dismissed.
- 5378: The requested credentials delegation was disallowed by policy.
- 5632: A request was made to authenticate to a wireless network.
- 5633: A request was made to authenticate to a wired network.

The recommended state for this setting is: **Success and Failure**.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using **auditpol.exe**, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce921c-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Success and Failure**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Other Logon/Logoff Events
```

Default Value:

No Auditing.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			
v7	16.13 Alert on Account Login Behavior Deviation Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			

17.5.6 Ensure 'Audit Special Logon' is set to include 'Success' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This subcategory reports when a special logon is used. A special logon is a logon that has administrator-equivalent privileges and can be used to elevate a process to a higher level. Events for this subcategory include:

- 4964: Special groups have been assigned to a new logon.

The recommended state for this setting is to include: **Success**.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using **auditpol.exe**, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce921b-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to include **Success**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Special Logon
```

Default Value:

Success.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224895
Rule ID: SV-224895r569186_rule
STIG ID: WN16-AU-000280
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●
v7	16.13 Alert on Account Login Behavior Deviation Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

17.6 Object Access

This section contains recommendations for configuring the Object Access audit policy.

17.6.1 Ensure 'Audit Detailed File Share' is set to include 'Failure' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory allows you to audit attempts to access files and folders on a shared folder. Events for this subcategory include:

- 5145: network share object was checked to see whether client can be granted desired access.

The recommended state for this setting is to include: **Failure**

Rationale:

Auditing the Failures will log which unauthorized users attempted (and failed) to get access to a file or folder on a network share on this computer, which could possibly be an indication of malicious intent.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using **auditpol.exe**, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9244-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to include **Failure**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Object Access\Audit Detailed File Share
```

Default Value:

No Auditing.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

17.6.2 Ensure 'Audit File Share' is set to 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to audit attempts to access a shared folder.

The recommended state for this setting is: **Success and Failure**.

Note: There are no system access control lists (SACLs) for shared folders. If this policy setting is enabled, access to all shared folders on the system is audited.

Rationale:

In an enterprise managed environment, it's important to track deletion, creation, modification, and access events for network shares. Any unusual file sharing activity may be useful in an investigation of potentially malicious activity.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using **auditpol.exe**, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9224-69ae-11d9-bed3-505054503030}"
```


Remediation:

To establish the recommended configuration via GP, set the following UI path to **Success and Failure**:

Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Object Access\Audit File Share

Default Value:

No Auditing.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			
v7	14.6 <u>Protect Information through Access Control Lists</u> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

17.6.3 Ensure 'Audit Other Object Access Events' is set to 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting allows you to audit events generated by the management of task scheduler jobs or COM+ objects.

For scheduler jobs, the following are audited:

- Job created.
- Job deleted.
- Job enabled.
- Job disabled.
- Job updated.

For COM+ objects, the following are audited:

- Catalog object added.
- Catalog object updated.
- Catalog object deleted.

The recommended state for this setting is: **Success and Failure**.

Rationale:

The unexpected creation of scheduled tasks and COM+ objects could potentially be an indication of malicious activity. Since these types of actions are generally low volume, it may be useful to capture them in the audit logs for use during an investigation.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using **auditpol.exe**, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9227-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Success and Failure**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Object Access\Audit Other Object Access Events
```

Default Value:

No Auditing.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224896 and V-224897
Rule ID: SV-224896r569186_rule and SV-224897r569186_rule
STIG ID: WN16-AU-000285 and WN16-AU-000286
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

17.6.4 Ensure 'Audit Removable Storage' is set to 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting allows you to audit user attempts to access file system objects on a removable storage device. A security audit event is generated only for all objects for all types of access requested. If you configure this policy setting, an audit event is generated each time an account accesses a file system object on a removable storage. Success audits record successful attempts and Failure audits record unsuccessful attempts. If you do not configure this policy setting, no audit event is generated when an account accesses a file system object on a removable storage.

The recommended state for this setting is: **Success and Failure**.

Note: A Windows 8.0, Server 2012 (non-R2) or newer OS is required to access and set this value in Group Policy.

Rationale:

Auditing removable storage may be useful when investigating an incident. For example, if an individual is suspected of copying sensitive information onto a USB drive.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using **auditpol.exe**, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9245-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Success and Failure**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Object Access\Audit Removable Storage
```

Default Value:

No Auditing.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224898 and V-224899
Rule ID: SV-224898r569186_rule and SV-224899r569186_rule
STIG ID: WN16-AU-000290 and WN16-AU-000300
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

17.7 Policy Change

This section contains recommendations for configuring the Policy Change audit policy.

17.7.1 Ensure 'Audit Audit Policy Change' is set to include 'Success' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports changes in audit policy including SACL changes. Events for this subcategory include:

- 4715: The audit policy (SACL) on an object was changed.
- 4719: System audit policy was changed.
- 4902: The Per-user audit policy table was created.
- 4904: An attempt was made to register a security event source.
- 4905: An attempt was made to unregister a security event source.
- 4906: The CrashOnAuditFail value has changed.
- 4907: Auditing settings on object were changed.
- 4908: Special Groups Logon table modified.
- 4912: Per User Audit Policy was changed.

The recommended state for this setting is include: **Success**.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using **auditpol.exe**, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce922f-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to include **Success**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change\Audit Audit Policy Change
```

Default Value:

Success.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

17.7.2 Ensure 'Audit Audit Policy Change' is set to include 'Success and Failure' (STIG only) (Automated)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This subcategory reports changes in audit policy including SACL changes. Events for this subcategory include:

- 4715: The audit policy (SACL) on an object was changed.
- 4719: System audit policy was changed.
- 4902: The Per-user audit policy table was created.
- 4904: An attempt was made to register a security event source.
- 4905: An attempt was made to unregister a security event source.
- 4906: The CrashOnAuditFail value has changed.
- 4907: Auditing settings on object were changed.
- 4908: Special Groups Logon table modified.
- 4912: Per User Audit Policy was changed.

The recommended state for this setting is include: **Success**.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to include **Success** and **Failure**:

Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change\Audit Audit Policy Change

Default Value:

Success.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224900 and V-224901
Rule ID: SV-224900r852310_rule and SV-224901r852311_rule
STIG ID: WN16-AU-000310 and WN16-AU-000320
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

17.7.3 Ensure 'Audit Authentication Policy Change' is set to include 'Success' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This subcategory reports changes in authentication policy. Events for this subcategory include:

- 4706: A new trust was created to a domain.
- 4707: A trust to a domain was removed.
- 4713: Kerberos policy was changed.
- 4716: Trusted domain information was modified.
- 4717: System security access was granted to an account.
- 4718: System security access was removed from an account.
- 4739: Domain Policy was changed.
- 4864: A namespace collision was detected.
- 4865: A trusted forest information entry was added.
- 4866: A trusted forest information entry was removed.
- 4867: A trusted forest information entry was modified.

The recommended state for this setting is to include: **Success**.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using **auditpol.exe**, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9230-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to include **Success:**

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change\Audit Authentication Policy Change
```

Default Value:

Success.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224902
Rule ID: SV-224902r852312_rule
STIG ID: WN16-AU-000330
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

17.7.4 Ensure 'Audit Authorization Policy Change' is set to include 'Success' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This subcategory reports changes in authorization policy. Events for this subcategory include:

- 4703: A user right was adjusted.
- 4704: A user right was assigned.
- 4705: A user right was removed.
- 4670: Permissions on an object were changed.
- 4911: Resource attributes of the object were changed.
- 4913: Central Access Policy on the object was changed.

The recommended state for this setting is to include: **Success**.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using **auditpol.exe**, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9231-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to include **Success**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change\Audit Authorization Policy Change
```

Default Value:

Success.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224903
Rule ID: SV-224903r852313_rule
STIG ID: WN16-AU-000340
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	5.5 <u>Implement Automated Configuration Monitoring Systems</u> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

17.7.5 Ensure 'Audit MPSSVC Rule-Level Policy Change' is set to 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory determines whether the operating system generates audit events when changes are made to policy rules for the Microsoft Protection Service (MPSSVC.exe). Events for this subcategory include:

- 4944: The following policy was active when the Windows Firewall started.
- 4945: A rule was listed when the Windows Firewall started.
- 4946: A change has been made to Windows Firewall exception list. A rule was added.
- 4947: A change has been made to Windows Firewall exception list. A rule was modified.
- 4948: A change has been made to Windows Firewall exception list. A rule was deleted.
- 4949: Windows Firewall settings were restored to the default values.
- 4950: A Windows Firewall setting has changed.
- 4951: A rule has been ignored because its major version number was not recognized by Windows Firewall.
- 4952: Parts of a rule have been ignored because its minor version number was not recognized by Windows Firewall. The other parts of the rule will be enforced.
- 4953: A rule has been ignored by Windows Firewall because it could not parse the rule.
- 4954: Windows Firewall Group Policy settings have changed. The new settings have been applied.
- 4956: Windows Firewall has changed the active profile.
- 4957: Windows Firewall did not apply the following rule.
- 4958: Windows Firewall did not apply the following rule because the rule referred to items not configured on this computer.

The recommended state for this setting is: **Success and Failure**

Rationale:

Changes to firewall rules are important for understanding the security state of the computer and how well it is protected against network attacks.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using **auditpol.exe**, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9232-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to

Success and Failure:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change\Audit MPSSVC Rule-Level Policy Change
```

Default Value:

No Auditing.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

17.7.6 Ensure 'Audit Other Policy Change Events' is set to include 'Failure' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory contains events about EFS Data Recovery Agent policy changes, changes in Windows Filtering Platform filter, status on Security policy settings updates for local Group Policy settings, Central Access Policy changes, and detailed troubleshooting events for Cryptographic Next Generation (CNG) operations.

- 5063: A cryptographic provider operation was attempted.
- 5064: A cryptographic context operation was attempted.
- 5065: A cryptographic context modification was attempted.
- 5066: A cryptographic function operation was attempted.
- 5067: A cryptographic function modification was attempted.
- 5068: A cryptographic function provider operation was attempted.
- 5069: A cryptographic function property operation was attempted.
- 5070: A cryptographic function property modification was attempted.
- 6145: One or more errors occurred while processing security policy in the group policy objects.

The recommended state for this setting is to include: **Failure**.

Rationale:

This setting can help detect errors in applied Security settings which came from Group Policy, and failure events related to Cryptographic Next Generation (CNG) functions.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using **auditpol.exe**, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9234-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to include **Failure**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change\Audit Other Policy Change Events
```

Default Value:

No Auditing.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

17.8 Privilege Use

This section contains recommendations for configuring the Privilege Use audit policy.

17.8.1 Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This subcategory reports when a user account or service uses a sensitive privilege. A sensitive privilege includes the following user rights:

- Act as part of the operating system
- Back up files and directories
- Create a token object
- Debug programs
- Enable computer and user accounts to be trusted for delegation
- Generate security audits
- Impersonate a client after authentication
- Load and unload device drivers
- Manage auditing and security log
- Modify firmware environment values
- Replace a process-level token
- Restore files and directories
- Take ownership of files or other objects

Auditing this subcategory will create a high volume of events. Events for this subcategory include:

- 4672: Special privileges assigned to new logon.
- 4673: A privileged service was called.
- 4674: An operation was attempted on a privileged object.

The recommended state for this setting is: **Success and Failure**.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using **auditpol.exe**, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9228-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to

Success and Failure:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced  
Audit Policy Configuration\Audit Policies\Privilege Use\Audit Sensitive  
Privilege Use
```

Default Value:

No Auditing.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224904 and V-224905
Rule ID: SV-224904r852314_rule and SV-224905r852315_rule
STIG ID: WN16-AU-000350 and WN16-AU-000360
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

17.9 System

This section contains recommendations for configuring the System audit policy.

17.9.1 Ensure 'Audit IPsec Driver' is set to 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This subcategory reports on the activities of the Internet Protocol security (IPsec) driver. Events for this subcategory include:

- 4960: IPsec dropped an inbound packet that failed an integrity check. If this problem persists, it could indicate a network issue or that packets are being modified in transit to this computer. Verify that the packets sent from the remote computer are the same as those received by this computer. This error might also indicate interoperability problems with other IPsec implementations.
- 4961: IPsec dropped an inbound packet that failed a replay check. If this problem persists, it could indicate a replay attack against this computer.
- 4962: IPsec dropped an inbound packet that failed a replay check. The inbound packet had too low a sequence number to ensure it was not a replay.
- 4963: IPsec dropped an inbound clear text packet that should have been secured. This is usually due to the remote computer changing its IPsec policy without informing this computer. This could also be a spoofing attack attempt.
- 4965: IPsec received a packet from a remote computer with an incorrect Security Parameter Index (SPI). This is usually caused by malfunctioning hardware that is corrupting packets. If these errors persist, verify that the packets sent from the remote computer are the same as those received by this computer. This error may also indicate interoperability problems with other IPsec implementations. In that case, if connectivity is not impeded, then these events can be ignored.
- 5478: IPsec Services has started successfully.
- 5479: IPsec Services has been shut down successfully. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks.
- 5480: IPsec Services failed to get the complete list of network interfaces on the computer. This poses a potential security risk because some of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem.
- 5483: IPsec Services failed to initialize RPC server. IPsec Services could not be started.

- 5484: IPsec Services has experienced a critical failure and has been shut down. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks.
- 5485: IPsec Services failed to process some IPsec filters on a plug-and-play event for network interfaces. This poses a potential security risk because some of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem.

The recommended state for this setting is: **Success and Failure**.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using **auditpol.exe**, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9213-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Success and Failure**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit IPsec Driver
```

Default Value:

No Auditing.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224906 and V-224907
Rule ID: SV-224906r852316_rule and SV-224907r852317_rule
STIG ID: WN16-AU-000370 and WN16-AU-000380
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

17.9.2 Ensure 'Audit Other System Events' is set to 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This subcategory reports on other system events. Events for this subcategory include:

- 5024: The Windows Firewall Service has started successfully.
- 5025: The Windows Firewall Service has been stopped.
- 5027: The Windows Firewall Service was unable to retrieve the security policy from the local storage. The service will continue enforcing the current policy.
- 5028: The Windows Firewall Service was unable to parse the new security policy. The service will continue with currently enforced policy.
- 5029: The Windows Firewall Service failed to initialize the driver. The service will continue to enforce the current policy.
- 5030: The Windows Firewall Service failed to start.
- 5032: Windows Firewall was unable to notify the user that it blocked an application from accepting incoming connections on the network.
- 5033: The Windows Firewall Driver has started successfully.
- 5034: The Windows Firewall Driver has been stopped.
- 5035: The Windows Firewall Driver failed to start.
- 5037: The Windows Firewall Driver detected critical runtime error. Terminating.
- 5058: Key file operation.
- 5059: Key migration operation.

The recommended state for this setting is: **Success and Failure**.

Rationale:

Capturing these audit events may be useful for identifying when the Windows Firewall is not performing as expected.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using **auditpol.exe**, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9214-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to

Success and Failure:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced  
Audit Policy Configuration\Audit Policies\System\Audit Other System Events
```

Default Value:

Success and Failure.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224908 and V-224909
Rule ID: SV-224908r852318_rule and SV-224909r852319_rule
STIG ID: WN16-AU-000390 and WN16-AU-000400
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

17.9.3 Ensure 'Audit Security State Change' is set to include 'Success' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This subcategory reports changes in security state of the system, such as when the security subsystem starts and stops. Events for this subcategory include:

- 4608: Windows is starting up.
- 4609: Windows is shutting down.
- 4616: The system time was changed.
- 4621: Administrator recovered system from CrashOnAuditFail. Users who are not administrators will now be allowed to log on. Some auditable activity might not have been recorded.

The recommended state for this setting is to include: **Success**.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using **auditpol.exe**, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9210-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to include **Success**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit Security State Change
```

Default Value:

Success.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224910
Rule ID: SV-224910r852320_rule
STIG ID: WN16-AU-000410
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

17.9.4 Ensure 'Audit Security System Extension' is set to include 'Success' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This subcategory reports the loading of extension code such as authentication packages by the security subsystem. Events for this subcategory include:

- 4610: An authentication package has been loaded by the Local Security Authority.
- 4611: A trusted logon process has been registered with the Local Security Authority.
- 4614: A notification package has been loaded by the Security Account Manager.
- 4622: A security package has been loaded by the Local Security Authority.
- 4697: A service was installed in the system.

The recommended state for this setting is to include: **Success**.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using **auditpol.exe**, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9211-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to include **Success**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit Security System Extension
```

Default Value:

No Auditing.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224911
Rule ID: SV-224911r852321_rule
STIG ID: WN16-AU-000420
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

17.9.5 Ensure 'Audit System Integrity' is set to 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This subcategory reports on violations of integrity of the security subsystem. Events for this subcategory include:

- 4612: Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits.
- 4615: Invalid use of LPC port.
- 4618: A monitored security event pattern has occurred.
- 4816: RPC detected an integrity violation while decrypting an incoming message.
- 5038: Code integrity determined that the image hash of a file is not valid. The file could be corrupt due to unauthorized modification or the invalid hash could indicate a potential disk device error.
- 5056: A cryptographic self test was performed.
- 5057: A cryptographic primitive operation failed.
- 5060: Verification operation failed.
- 5061: Cryptographic operation.
- 5062: A kernel-mode cryptographic self test was performed.

The recommended state for this setting is: **Success and Failure**.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using **auditpol.exe**, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9212-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Success and Failure**:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit System Integrity
```

Default Value:

Success and Failure.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224912 and V-224913
Rule ID: SV-224912r852322_rule and SV-224913r852323_rule
STIG ID: WN16-AU-000440 and WN16-AU-000450
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

18 Administrative Templates (Computer)

This section contains computer-based recommendations from Group Policy Administrative Templates (ADMX).

18.1 Control Panel

This section contains recommendations for Control Panel settings.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.1.1 Personalization

This section contains recommendations for Control Panel personalization settings.

This Group Policy section is provided by the Group Policy template `ControlPanelDisplay.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.1.1.1 Ensure 'Prevent enabling lock screen camera' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Disables the lock screen camera toggle switch in PC Settings and prevents a camera from being invoked on the lock screen.

The recommended state for this setting is: **Enabled**.

Rationale:

Disabling the lock screen camera extends the protection afforded by the lock screen to camera features.

Impact:

If you enable this setting, users will no longer be able to enable or disable lock screen camera access in PC Settings, and the camera cannot be invoked on the lock screen.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Personalization:NoLockScreenCamera
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\Control  
Panel\Personalization\Prevent enabling lock screen camera
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **ControlPanelDisplay.admx/adml** that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Disabled. (Users can enable invocation of an available camera on the lock screen.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

18.1.1.2 Ensure 'Prevent enabling lock screen slide show' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

Disables the lock screen slide show settings in PC Settings and prevents a slide show from playing on the lock screen.

The recommended state for this setting is: **Enabled**.

Rationale:

Disabling the lock screen slide show extends the protection afforded by the lock screen to slide show contents.

Impact:

If you enable this setting, users will no longer be able to modify slide show settings in PC Settings, and no slide show will ever start.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Personalization:NoLockScreenSlideshow
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\Control Panel\Personalization\Prevent enabling lock screen slide show
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **ControlPanelDisplay.admx/adml** that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Disabled. (Users can enable a slide show that will run after they lock the machine.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224914
Rule ID: SV-224914r569186_rule
STIG ID: WN16-CC-000010
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

18.1.2 Regional and Language Options

This section contains recommendation settings for Regional and Language Options.

This Group Policy section is provided by the Group Policy template [Globalization.admx/adml](#) that is included with all versions of the Microsoft Windows Administrative Templates.

18.1.2.1 Handwriting personalization

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template [Globalization.admx/adml](#) that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.1.2.2 Ensure 'Allow users to enable online speech recognition services' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy enables the automatic learning component of input personalization that includes speech, inking, and typing. Automatic learning enables the collection of speech and handwriting patterns, typing history, contacts, and recent calendar information. It is required for the use of Cortana. Some of this collected information may be stored on the user's OneDrive, in the case of inking and typing; some of the information will be uploaded to Microsoft to personalize speech.

The recommended state for this setting is: **Disabled**.

Rationale:

If this setting is Enabled sensitive information could be stored in the cloud or sent to Microsoft.

Impact:

Automatic learning of speech, inking, and typing stops and users cannot change its value via PC Settings.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

HKLM\SOFTWARE\Policies\Microsoft\InputPersonalization:AllowInputPersonalization

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

Computer Configuration\Policies\Administrative Templates\Control Panel\Regional and Language Options\Allow users to enable online speech recognition services

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **Globalization.admx/adml** that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Allow input personalization*, but it was renamed to *Allow users to enable online speech recognition services* starting with the Windows 10 R1809 & Server 2019 Administrative Templates.

Default Value:

Enabled. (Automatic learning of speech, inking and typing is enabled, but users may change this value via PC Settings.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

18.1.3 Ensure 'Allow Online Tips' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting configures the retrieval of online tips and help for the Settings app.

The recommended state for this setting is: **Disabled**.

Rationale:

Due to privacy concerns, data should never be sent to any third-party since this data could contain sensitive information.

Impact:

Settings will not contact Microsoft content services to retrieve tips and help content.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer:AllowOnlineTips
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Administrative Templates\Control Panel\Allow Online Tips
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **ControlPanel.admx/adml** that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Default Value:

Enabled. (Settings will contact Microsoft content services to retrieve tips and help content.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●
v7	9.3 <u>Perform Regular Automated Port Scans</u> Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.		●	●

18.2 Desktop

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template [Desktop.admx/adml](#) that is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v1.0 (or newer).

18.3 LAPS (legacy)

This section contains recommendations for configuring legacy Microsoft Local Administrator Password Solution (LAPS). This older version of LAPS is still applicable to Windows Server 2016, which is not supported by the newer Windows LAPS.

This Group Policy section is provided by the Group Policy template [AdmPwd.admx/adml](#) that is included with older versions of the [Microsoft Security Compliance Toolkit and Baselines](#). Regardless of Windows Operating System version, download the Security Baseline for Windows 11 22H2, which is the last Security Baseline to obtain the template.

Legacy Microsoft LAPS can be downloaded from [Download LAPS from Official Microsoft Download Center](#).

18.3.1 Ensure LAPS AdmPwd GPO Extension / CSE is installed (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server
- STIG Member Server

Description:

In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and Member Servers. The passwords are stored in a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed.

The LAPS tool requires a small Active Directory Schema update in order to implement, as well as installation of a Group Policy Client Side Extension (CSE) on targeted computers. Please see the LAPS documentation for details.

LAPS supports Windows Vista or newer workstation OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain.

Note: Organizations that utilize third-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

Note #2: LAPS is only designed to manage *local* Administrator passwords, and is therefore not recommended (or supported) for use directly on Domain Controllers, which do not have a traditional local Administrator account. We strongly encourage you to only deploy the LAPS CSE and LAPS GPO settings to member servers and workstations.

Rationale:

Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or Member Servers when deploying them. This creates a serious attack surface security risk because if an attacker manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account.

Impact:

No impact. When installed and registered properly, **AdmPwd.dll** takes no action unless given appropriate GPO commands during Group Policy refresh. It is not a memory-resident agent or service.

In a disaster recovery scenario where Active Directory is not available, the local Administrator password will not be retrievable and a local password reset using a tool (such as Microsoft's Disaster and Recovery Toolset (DaRT) Recovery Image) may be necessary.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_SZ** value of **C:\Program Files\LAPS\CSE\AdmPwd.dll** or **C:\Program Files\LAPS\CSE\AdmPwd.dll**.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\Winlogon\GPExtensions\{D76B9641-3288-4f75-942D-  
087DE603E3EA}:DllName
```

Remediation:

In order to utilize LAPS, a minor Active Directory Schema update is required, and a Group Policy Client Side Extension (CSE) must be installed on each managed computer. When LAPS is installed, the file **AdmPwd.dll** must be present in the following location and registered in Windows (the LAPS AdmPwd GPO Extension / CSE installation does this for you):

```
C:\Program Files\LAPS\CSE\AdmPwd.dll
```

Default Value:

Not Installed.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224820
Rule ID: SV-224820r857224_rule
STIG ID: WN16-00-000030
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.			
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			
v7	16.2 Configure Centralized Point of Authentication Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.			

18.3.2 Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and Member Servers. The passwords are stored in a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed.

The LAPS tool requires a small Active Directory Schema update in order to implement, as well as installation of a Group Policy Client Side Extension (CSE) on targeted computers. Please see the LAPS documentation for details.

LAPS supports Windows Vista or newer workstation OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain.

The recommended state for this setting is: **Enabled**.

Note: Organizations that utilize third-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

Note #2: LAPS is only designed to manage *local* Administrator passwords, and is therefore not recommended (or supported) for use directly on Domain Controllers, which do not have a traditional local Administrator account. We strongly encourage you to only deploy the LAPS CSE and LAPS GPO settings to member servers and workstations.

Note #2: LAPS is only designed to manage *local* Administrator passwords, and is therefore not recommended (or supported) for use directly on Domain Controllers, which do not have a traditional local Administrator account. We strongly encourage you to only deploy the LAPS CSE and LAPS GPO settings to member servers and workstations.

Rationale:

Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or Member Servers when deploying them. This creates a serious attack surface security risk because if an attacker manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account.

Impact:

Planned password expiration longer than password age dictated by "Password Settings" policy is NOT allowed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft  
Services\AdmPwd:PwdExpirationProtectionEnabled
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\LAPS\Do not allow  
password expiration time longer than required by policy
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (**AdmPwd.admx/adm1**) is required - it is included with Microsoft Local Administrator Password Solution (LAPS).

Default Value:

Disabled. (Password expiration time may be longer than required by the "Password Settings" policy.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	16.10 <u>Ensure All Accounts Have An Expiration Date</u> Ensure that all accounts have an expiration date that is monitored and enforced.		●	●

18.3.3 Ensure 'Enable Local Admin Password Management' is set to 'Enabled' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and Member Servers. The passwords are stored in a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed.

The LAPS tool requires a small Active Directory Schema update in order to implement, as well as installation of a Group Policy Client Side Extension (CSE) on targeted computers. Please see the LAPS documentation for details.

LAPS supports Windows Vista or newer workstation OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain.

The recommended state for this setting is: **Enabled**.

Note: Organizations that utilize 3rd-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

Note #2: LAPS is only designed to manage *local* Administrator passwords, and is therefore not recommended (or supported) for use directly on Domain Controllers, which do not have a traditional local Administrator account. We strongly encourage you to only deploy the LAPS CSE and LAPS GPO settings to member servers and workstations.

Rationale:

Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or Member Servers when deploying them. This creates a serious attack surface security risk because if an attacker manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account.

Impact:

The local administrator password is managed (provided that the LAPS AdmPwd GPO Extension / CSE is installed on the target computer (see recommendation *Ensure LAPS AdmPwd GPO Extension / CSE is installed*), the Active Directory domain schema and account permissions have been properly configured on the domain).

In a disaster recovery scenario where Active Directory is not available, the local Administrator password will not be retrievable and a local password reset using a tool (such as Microsoft's Disaster and Recovery Toolset (DaRT) Recovery Image) may be necessary.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft Services\AdmPwd:AdmPwdEnabled
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\LAPS\Enable Local Admin Password Management
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (**AdmPwd.admx/adml**) is required - it is included with Microsoft Local Administrator Password Solution (LAPS).

Default Value:

Disabled. (Local Administrator password is NOT managed.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 <u>Use Unique Passwords</u> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v8	5.4 <u>Restrict Administrator Privileges to Dedicated Administrator Accounts</u> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.			
v7	4.4 <u>Use Unique Passwords</u> Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			
v7	16.2 <u>Configure Centralized Point of Authentication</u> Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.			

18.3.4 Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + special characters' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and Member Servers. The passwords are stored in a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed.

The LAPS tool requires a small Active Directory Schema update in order to implement, as well as installation of a Group Policy Client Side Extension (CSE) on targeted computers. Please see the LAPS documentation for details.

LAPS supports Windows Vista or newer workstation OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain.

The recommended state for this setting is: **Enabled: Large letters + small letters + numbers + special characters.**

Note: Organizations that utilize 3rd-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

Note #2: LAPS is only designed to manage *local* Administrator passwords, and is therefore not recommended (or supported) for use directly on Domain Controllers, which do not have a traditional local Administrator account. We strongly encourage you to only deploy the LAPS CSE and LAPS GPO settings to member servers and workstations.

Rationale:

Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or Member Servers when deploying them. This creates a serious attack surface security risk because if an attacker manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **4**.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft  
Services\AdmPwd>PasswordComplexity
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**, and configure the **Password Complexity** option to **Large letters + small letters + numbers + special characters**:

```
Computer Configuration\Policies\Administrative Templates\LAPS>Password  
Settings
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (**AdmPwd.admx/adml**) is required - it is included with Microsoft Local Administrator Password Solution (LAPS).

Default Value:

Large letters + small letters + numbers + special characters.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			

18.3.5 Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and Member Servers. The passwords are stored in a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed.

The LAPS tool requires a small Active Directory Schema update in order to implement, as well as installation of a Group Policy Client Side Extension (CSE) on targeted computers. Please see the LAPS documentation for details.

LAPS supports Windows Vista or newer workstation OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain.

The recommended state for this setting is: **Enabled: 15 or more.**

Note: Organizations that utilize 3rd-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

Note #2: LAPS is only designed to manage *local* Administrator passwords, and is therefore not recommended (or supported) for use directly on Domain Controllers, which do not have a traditional local Administrator account. We strongly encourage you to only deploy the LAPS CSE and LAPS GPO settings to member servers and workstations.

Rationale:

Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or Member Servers when deploying them. This creates a serious attack surface security risk because if an attacker manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account.

Impact:

LAPS-generated passwords will be required to have a length of 15 characters (or more, if selected).

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **15** or more.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft Services\AdmPwd>PasswordLength

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**, and configure the **Password Length** option to **15 or more**:

Computer Configuration\Policies\Administrative Templates\LAPS>Password Settings

Note: This Group Policy path does not exist by default. An additional Group Policy template (**AdmPwd.admx/adml**) is required - it is included with Microsoft Local Administrator Password Solution (LAPS).

Default Value:

14 characters.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			

18.3.6 Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and Member Servers. The passwords are stored in a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed.

The LAPS tool requires a small Active Directory Schema update in order to implement, as well as installation of a Group Policy Client Side Extension (CSE) on targeted computers. Please see the LAPS documentation for details.

LAPS supports Windows Vista or newer workstation OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain.

The recommended state for this setting is: **Enabled: 30 or fewer**.

Note: Organizations that utilize 3rd-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

Note #2: LAPS is only designed to manage *local* Administrator passwords, and is therefore not recommended (or supported) for use directly on Domain Controllers, which do not have a traditional local Administrator account. We strongly encourage you to only deploy the LAPS CSE and LAPS GPO settings to member servers and workstations.

Rationale:

Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or Member Servers when deploying them. This creates a serious attack surface security risk because if an attacker manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account.

Impact:

None - this is the default behavior, unless set to fewer than 30 days.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **30** or less.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft  
Services\AdmPwd>PasswordAgeDays
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**, and configure the **Password Age (Days)** option to **30 or fewer**:

```
Computer Configuration\Policies\Administrative Templates\LAPS>Password  
Settings
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (**AdmPwd.admx/adml**) is required - it is included with Microsoft Local Administrator Password Solution (LAPS).

Default Value:

30 days.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v7	16.10 Ensure All Accounts Have An Expiration Date Ensure that all accounts have an expiration date that is monitored and enforced.			

18.3.7 Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 60 or fewer' (STIG MS only) (Automated)

Profile Applicability:

- STIG Member Server

Description:

In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and Member Servers. The passwords are stored in a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed.

The LAPS tool requires a small Active Directory Schema update in order to implement, as well as installation of a Group Policy Client Side Extension (CSE) on targeted computers. Please see the LAPS documentation for details.

LAPS supports Windows Vista or newer workstation OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain.

The recommended state for this setting is: **Enabled: 60 or fewer**.

Note: Organizations that utilize 3rd-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

Note #2: LAPS is only designed to manage *local* Administrator passwords and is therefore not recommended (or supported) for use directly on Domain Controllers, which do not have a traditional local Administrator account. We strongly encourage you to only deploy the LAPS CSE and LAPS GPO settings to member servers and workstations.

Rationale:

Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or Member Servers when deploying them. This creates a serious attack surface security risk because if an attacker manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account.

Impact:

LAPS-generated passwords will be required to have a maximum age of 30 days (or fewer, if selected).

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **60**.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft  
Services\AdmPwd>PasswordAgeDays
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**, and configure the **Password Age (Days)** option to **60 or fewer**:

```
Computer Configuration\Policies\Administrative Templates\LAPS>Password  
Settings
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (**AdmPwd.admx/adml**) is required - it is included with Microsoft Local Administrator Password Solution (LAPS).

Default Value:

30 days.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224820
Rule ID: SV-224820r857224_rule
STIG ID: WN16-00-000030
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	16.10 Ensure All Accounts Have An Expiration Date Ensure that all accounts have an expiration date that is monitored and enforced.		●	●

18.4 MS Security Guide

This section contains recommendations for configuring additional settings from the MS Security Guide.

This Group Policy section is provided by the Group Policy template `SecGuide.admx/adml` that is available for download from the [Microsoft Security Compliance Toolkit and Baselines](#) website. Regardless of Windows Operating System version, download the latest Windows 11 Security Baseline to obtain the template.

18.4.1 Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server
- STIG Member Server

Description:

This setting controls whether local accounts can be used for remote administration via network logon (e.g., NET USE, connecting to C\$, etc.). Local accounts are at high risk for credential theft when the same account and password is configured on multiple systems. Enabling this policy significantly reduces that risk.

Enabled: Applies UAC token-filtering to local accounts on network logons. Membership in powerful group such as Administrators is disabled and powerful privileges are removed from the resulting access token. This configures the **LocalAccountTokenFilterPolicy** registry value to **0**. This is the default behavior for Windows.

Disabled: Allows local accounts to have full administrative rights when authenticating via network logon, by configuring the **LocalAccountTokenFilterPolicy** registry value to **1**.

For more information about local accounts and credential theft, review the "[Mitigating Pass-the-Hash \(PtH\) Attacks and Other Credential Theft Techniques](#)" documents.

For more information about **LocalAccountTokenFilterPolicy**, see Microsoft Knowledge Base article 951016: [Description of User Account Control and remote restrictions in Windows Vista](#).

The recommended state for this setting is: **Enabled**.

Rationale:

Local accounts are at high risk for credential theft when the same account and password is configured on multiple systems. Ensuring this policy is Enabled significantly reduces that risk.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:LocalAccountTo  
kenFilterPolicy
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\MS Security  
Guide\Apply UAC restrictions to local accounts on network logons
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (**SecGuide.admx/adml**) is required - it is available from Microsoft at [this link](#).

Default Value:

Enabled. (UAC token-filtering is applied to local accounts on network logons. Membership in powerful groups such as Administrators and disabled and powerful privileges are removed from the resulting access token.)

Additional Information:

```
Microsoft Windows Server 2016 Security Technical Implementation Guide:  
Version 2, Release 6, Benchmark Date: May 11, 2023
```

```
Vul ID: V-225008  
Rule ID: SV-225008r857258_rule  
STIG ID: WN16-MS-000020  
Severity: CAT II
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	4.3 <u>Ensure the Use of Dedicated Administrative Accounts</u> Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●

18.4.2 Ensure 'Configure RPC packet level privacy setting for incoming connections' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls packet level privacy for Remote Procedure Call (RPC) incoming connections.

The recommended state for this setting is: **Enabled**.

Rationale:

A security bypass vulnerability ([CVE-2021-1678 | Windows Print Spooler Spoofing Vulnerability](#)) exists in the way the Printer RPC binding handles authentication for the remote Winspool interface. Enabling the RPC packet level privacy setting for incoming connections enforces the server-side to increase the authentication level to minimize this vulnerability.

Impact:

None - this is default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SYSTEM\CurrentControlSet\Control\Print:RpcAuthnLevelPrivacyEnabled
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\MS Security Guide\Configure RPC packet level privacy setting for incoming connections
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (**SecGuide.admx/adml**) is required - it is available from Microsoft at [this link](#).

Default Value:

Enabled. (Packet level privacy is enabled for RPC for incoming connections.)

References:

1. <https://support.microsoft.com/en-us/topic/managing-deployment-of-printer-rpc-binding-changes-for-cve-2021-1678-kb4599464-12a69652-30b9-3d61-d9f7-7201623a8b25>
2. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-1678>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

18.4.3 Ensure 'Configure SMB v1 client driver' is set to 'Enabled: Disable driver (recommended)' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This setting configures the start type for the Server Message Block version 1 (SMBv1) client driver service (**MRxSmb10**), which is recommended to be disabled.

The recommended state for this setting is: **Enabled: Disable driver (recommended)**.

Note: Do not, *under any circumstances*, configure this overall setting as **Disabled**, as doing so will delete the underlying registry entry altogether, which will cause serious problems.

Rationale:

Since September 2016, Microsoft has strongly encouraged that SMBv1 be disabled and no longer used on modern networks, as it is a 30 year old design that is much more vulnerable to attacks than much newer designs such as SMBv2 and SMBv3.

More information on this can be found at the following links:

[Stop using SMB1 | Storage at Microsoft](#)

[Disable SMB v1 in Managed Environments with Group Policy – "Stay Safe" Cyber Security Blog](#)

[Disabling SMBv1 through Group Policy – Microsoft Security Guidance blog](#)

Impact:

Some legacy OSes (e.g. Windows XP, Server 2003 or older), applications and appliances may no longer be able to communicate with the system once SMBv1 is disabled. We recommend careful testing be performed to determine the impact prior to configuring this as a widespread control, and where possible, remediate any incompatibilities found with the vendor of the incompatible system. Microsoft is also maintaining a thorough (although not comprehensive) list of known SMBv1 incompatibilities at this link: [SMB1 Product Clearinghouse | Storage at Microsoft](#)

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **4**.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\mrxsmb10:Start
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled: Disable driver (recommended)**:

```
Computer Configuration\Policies\Administrative Templates\MS Security  
Guide\Configure SMB v1 client driver
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (**SecGuide.admx/adml**) is required - it is available from Microsoft at [this link](#).

Default Value:

Windows Server 2008 (non-R2), 2008 R2, and 2012 (non-R2): Enabled: Manual start.

Windows Server 2012 R2 and Server 2016 (up to R1607): Enabled: Automatic start.

Windows Server 2016 R1709 or newer: Enabled: Disable driver.

Additional Information:

```
Microsoft Windows Server 2016 Security Technical Implementation Guide:  
Version 2, Release 8, Benchmark Date: May 15, 2024
```

```
Vul ID:    V-224858  
Rule ID:   SV-224858r569186_rule  
STIG ID:   WN16-00-000412  
Severity:  CAT II
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			
v7	<u>14.3 Disable Workstation to Workstation Communication</u> Disable all workstation to workstation communication to limit an attacker's ability to move laterally and compromise neighboring systems, through technologies such as Private VLANs or microsegmentation.			

18.4.4 Ensure 'Configure SMB v1 server' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This setting configures the server-side processing of the Server Message Block version 1 (SMBv1) protocol.

The recommended state for this setting is: **Disabled**.

Rationale:

Since September 2016, Microsoft has strongly encouraged that SMBv1 be disabled and no longer used on modern networks, as it is a 30 year old design that is much more vulnerable to attacks than much newer designs such as SMBv2 and SMBv3.

More information on this can be found at the following links:

[Stop using SMB1 | Storage at Microsoft](#)

[Disable SMB v1 in Managed Environments with Group Policy – "Stay Safe" Cyber Security Blog](#)

[Disabling SMBv1 through Group Policy – Microsoft Security Guidance blog](#)

Impact:

Some legacy OSes (e.g. Windows XP, Server 2003 or older), applications and appliances may no longer be able to communicate with the system once SMBv1 is disabled. We recommend careful testing be performed to determine the impact prior to configuring this as a widespread control, and where possible, remediate any incompatibilities found with the vendor of the incompatible system. Microsoft is also maintaining a thorough (although not comprehensive) list of known SMBv1 incompatibilities at this link: [SMB1 Product Clearinghouse | Storage at Microsoft](#)

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters:SMB1
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Administrative Templates\MS Security  
Guide\Configure SMB v1 server
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (**SecGuide.admx/adml**) is required - it is available from Microsoft at [this link](#).

Default Value:

Windows Server 2016 R1607 and older: Enabled.

Windows Server 2016 R1709 or newer: Disabled.

Additional Information:

```
Microsoft Windows Server 2016 Security Technical Implementation Guide:  
Version 2, Release 8, Benchmark Date: May 15, 2024
```

```
Vul ID:    V-224857  
Rule ID:   SV-224857r569186_rule  
STIG ID:   WN16-00-000411  
Severity:  CAT II
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			
v7	<u>14.3 Disable Workstation to Workstation Communication</u> Disable all workstation to workstation communication to limit an attacker's ability to move laterally and compromise neighboring systems, through technologies such as Private VLANs or microsegmentation.			

18.4.5 Ensure 'Enable Certificate Padding' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting configures whether the [WinVerifyTrust](#) function performs strict Windows Authenticode signature verification for Portable Executable files (PE files). If enabled, PE files will be considered "unsigned" if Windows identifies content in them that does not conform to the Authenticode specification.

The recommended state for this setting is: **Enabled**.

Rationale:

A remote code execution vulnerability exists in the way that the [WinVerifyTrust](#) function handles Windows Authenticode signature verification for portable executable (PE) files. For more information on this vulnerability, visit [CVE-2013-3900 - Security Update Guide - Microsoft - WinVerifyTrust Signature Validation Vulnerability](#).

Impact:

Microsoft recommends that installers are built to only extract content from validated portions of signed files. Some installers do not follow this guidance and therefore may be negatively impacted by this setting.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Microsoft\Cryptography\Wintrust\Config:EnableCertPaddingCheck
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\MS Security  
Guide\Enable Certificate Padding
```

Note: This Group Policy path does not exist by default. An additional Group Policy template ([SecGuide.admx/adml](#)) is required - it is available from Microsoft at [this link](#).

Default Value:

Disabled. (The [WinVerifyTrust](#) function does not perform strict Windows Authenticode signature verification for Portable Executable files (PE files).)

References:

1. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2013-3900>
2. <https://learn.microsoft.com/en-us/windows/win32/api/wintrust/nf-wintrust-winverifytrust>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

18.4.6 Ensure 'Enable Structured Exception Handling Overwrite Protection (SEHOP)' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Windows includes support for Structured Exception Handling Overwrite Protection (SEHOP). We recommend enabling this feature to improve the security profile of the computer.

The recommended state for this setting is: **Enabled**.

Rationale:

This feature is designed to block exploits that use the Structured Exception Handler (SEH) overwrite technique. This protection mechanism is provided at run-time. Therefore, it helps protect applications regardless of whether they have been compiled with the latest improvements, such as the /SAFESEH option.

Impact:

After you enable SEHOP, existing versions of Cygwin, Skype, and Armadillo-protected applications may not work correctly.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SYSTEM\CurrentControlSet\Control\Session  
Manager\kernel:DisableExceptionChainValidation
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\MS Security  
Guide\Enable Structured Exception Handling Overwrite Protection (SEHOP)
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (**SecGuide.admx/adml**) is required - it is available from Microsoft at [this link](#). More information is available at [MSKB 956607: How to enable Structured Exception Handling Overwrite Protection \(SEHOP\) in Windows operating systems](#)

Default Value:

Disabled for 32-bit processes.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 <u>Enable Anti-Exploitation Features</u> Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.			
v7	8.3 <u>Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies</u> Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.			

18.4.7 Ensure 'LSA Protection' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls whether the Local Security Authority Server Service (LSASS) process runs protected. The Local Security Authority (LSA), which includes the Local Security Authority Server Service (LSASS) process, validates users for local and remote sign-ins and enforces local security policies.

The recommended state for this setting is: **Enabled**.

Note: This setting only applies to Windows Server 2012 R2 (or newer) **except** for Windows Server 2022 (or newer). See policy setting *Configure LSASS to run as a protected process*.

Rationale:

The Windows Server 2012 R2 (or newer) provides additional protection for the LSA to prevent reading memory and code injection by non-protected processes. Enabling this setting provides added security for the credentials that LSA stores and manages.

Impact:

If additional LSA protection is enabled, Administrators will not be able to debug a custom LSA plugin. A debugger cannot be attached to LSASS when it's a protected process. In general, there's no supported way to debug a running protected process.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SYSTEM\CurrentControlSet\Control\Lsa:RunAsPPL
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\MS Security  
Guide\LSA Protection
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (**SecGuide.admx/adml**) is required - it is available from Microsoft at [this link](#).

Default Value:

Disabled. (The LSASS process run unprotected.)

References:

1. <https://learn.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/configuring-additional-lsa-protection>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

18.4.8 Ensure 'NetBT NodeType configuration' is set to 'Enabled: P-node (recommended)' (Automated)

Profile Applicability:

- Level 1 - Member Server
- Level 1 - Domain Controller

Description:

This setting determines which method NetBIOS over TCP/IP (NetBT) uses to register and resolve names. The available methods are:

- The B-node (broadcast) method only uses broadcasts.
- The P-node (point-to-point) method only uses name queries to a name server (WINS).
- The M-node (mixed) method broadcasts first, then queries a name server (WINS) if broadcast failed.
- The H-node (hybrid) method queries a name server (WINS) first, then broadcasts if the query failed.

The recommended state for this setting is: **Enabled: P-node (recommended)** (point-to-point).

Note: Resolution through LMHOSTS or DNS follows these methods. If the **NodeType** registry value is present, it overrides any **DhcpNodeType** registry value. If neither **NodeType** nor **DhcpNodeType** is present, the computer uses B-node (broadcast) if there are no WINS servers configured for the network, or H-node (hybrid) if there is at least one WINS server configured.

Rationale:

In order to help mitigate the risk of NetBIOS Name Service (NBT-NS) poisoning attacks, setting the node type to P-node (point-to-point) will prevent the system from sending out NetBIOS broadcasts.

Impact:

NetBIOS name resolution queries will require a defined and available WINS server for external NetBIOS name resolution. If a WINS server is not defined or not reachable, and the desired hostname is not defined in the local cache, local LMHOSTS or HOSTS files, NetBIOS name resolution will fail.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **2**.

HKLM\SYSTEM\CurrentControlSet\Services\NetBT\Parameters:NodeType

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled: P-node (recommended)**:

Computer Configuration\Policies\Administrative Templates\MS Security Guide\NetBT NodeType configuration

Note: This change does not take effect until the computer has been restarted.

Note #2: This Group Policy path does not exist by default. An additional Group Policy template (**SecGuide.admx/adml**) is required - it is available from Microsoft at [this link](#). Please note that this setting is **only** available in the *Security baseline (FINAL)* for *Windows 10 v1903 and Windows Server v1903* (or newer) release of **SecGuide.admx/adml**, so if you previously downloaded this template, you may need to update it from a newer Microsoft baseline to get this new *NetBT NodeType configuration* setting.

Default Value:

B-node (broadcast only) if a WINS server is not configured in NIC properties.

H-node (hybrid - point-to-point first, then broadcast) if a WINS server is configured in NIC properties.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

18.4.9 Ensure 'WDigest Authentication' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

When WDigest authentication is enabled, Lsass.exe retains a copy of the user's plaintext password in memory, where it can be at risk of theft. If this setting is not configured, WDigest authentication is disabled in Windows 8.1 and in Windows Server 2012 R2; it is enabled by default in earlier versions of Windows and Windows Server.

For more information about local accounts and credential theft, review the "[Mitigating Pass-the-Hash \(PtH\) Attacks and Other Credential Theft Techniques](#)" documents.

For more information about [UseLogonCredential](#), see Microsoft Knowledge Base article 2871997: [Microsoft Security Advisory Update to improve credentials protection and management May 13, 2014](#).

The recommended state for this setting is: **Disabled**.

Rationale:

Preventing the plaintext storage of credentials in memory may reduce opportunity for credential theft.

Impact:

None - this is also the default configuration for Server 2012 R2 or newer.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest:UseLogonCredential
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

Computer Configuration\Policies\Administrative Templates\MS Security Guide\WDigest Authentication (disabling may require KB2871997)

Note: This Group Policy path does not exist by default. An additional Group Policy template (**SecGuide.admx/adml**) is required - it is available from Microsoft at [this link](#).

Default Value:

On Server 2012 (non-R2) and older: Enabled. (Lsass.exe retains a copy of the user's plaintext password in memory, where it is at risk of theft.)

On Server 2012 R2 or newer: Disabled. (Lsass.exe does not retain a copy of the user's plaintext password in memory.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15 2024

Vul ID: V-224915
Rule ID: SV-224915r569186_rule
STIG ID: WN16-CC-000030
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 <u>Encrypt Sensitive Data at Rest</u> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
v7	16.4 <u>Encrypt or Hash all Authentication Credentials</u> Encrypt or hash with a salt all authentication credentials when stored.			

18.5 MSS (Legacy)

This section contains recommendations for the Microsoft Solutions for Security (MSS) settings.

This Group Policy section is provided by the Group Policy template **MSS-legacy.admx/adml** that is available for download from the [Microsoft Security Compliance Toolkit and Baselines](#) website. Regardless of Windows Operating System version, download the latest Windows 11 Security Baseline to obtain the template.

18.5.1 Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This setting is separate from the Welcome screen feature in Windows XP and Windows Vista; if that feature is disabled, this setting is not disabled. If you configure a computer for automatic logon, anyone who can physically gain access to the computer can also gain access to everything that is on the computer, including any network or networks to which the computer is connected. Also, if you enable automatic logon, the password is stored in the registry in plaintext, and the specific registry key that stores this value is remotely readable by the Authenticated Users group.

For additional information, see Microsoft Knowledge Base article 324737: [How to turn on automatic logon in Windows](#).

The recommended state for this setting is: **Disabled**.

Rationale:

If you configure a computer for automatic logon, anyone who can physically gain access to the computer can also gain access to everything that is on the computer, including any network or networks that the computer is connected to. Also, if you enable automatic logon, the password is stored in the registry in plaintext. The specific registry key that stores this setting is remotely readable by the Authenticated Users group. As a result, this entry is appropriate only if the computer is physically secured and if you ensure that untrusted users cannot remotely see the registry.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_SZ** value of **0**.

```
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon:AutoAdminLogon
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS:
(AutoAdminLogon) Enable Automatic Logon

Note: This Group Policy path does not exist by default. An additional Group Policy template (**MSS-legacy.admx/adml**) is required - it is available from this TechNet blog post: [The MSS settings – Microsoft Security Guidance blog](#)

Default Value:

Disabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 <u>Encrypt Sensitive Data at Rest</u> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	16.4 <u>Encrypt or Hash all Authentication Credentials</u> Encrypt or hash with a salt all authentication credentials when stored.		●	●

18.5.2 Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level' is set to 'Enabled: Highest protection, source routing is completely disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

IP source routing is a mechanism that allows the sender to determine the IP route that a datagram should follow through the network.

The recommended state for this setting is: **Enabled: Highest protection, source routing is completely disabled.**

Rationale:

An attacker could use source routed packets to obscure their identity and location. Source routing allows a computer that sends a packet to specify the route that the packet takes.

Impact:

All incoming source routed packets will be dropped.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **2**.

```
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters\DisableIPSourceRouting
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled: Highest protection, source routing is completely disabled:**

Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS:
(DisableIPSourceRouting IPv6) IP source routing protection level

Note: This Group Policy path does not exist by default. An additional Group Policy template (**MSS-legacy.admx/adml**) is required - it is available from this TechNet blog post: [The MSS settings – Microsoft Security Guidance blog](#)

Default Value:

No additional protection, source routed packets are allowed.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224916
Rule ID: SV-224916r569186_rule
STIG ID: WN16-CC-000040
Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

18.5.3 Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level' is set to 'Enabled: Highest protection, source routing is completely disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

IP source routing is a mechanism that allows the sender to determine the IP route that a datagram should take through the network. It is recommended to configure this setting to Not Defined for enterprise environments and to Highest Protection for high security environments to completely disable source routing.

The recommended state for this setting is: **Enabled: Highest protection, source routing is completely disabled.**

Rationale:

An attacker could use source routed packets to obscure their identity and location. Source routing allows a computer that sends a packet to specify the route that the packet takes.

Impact:

All incoming source routed packets will be dropped.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **2**.

```
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters:DisableIPSourceRouting
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled: Highest protection, source routing is completely disabled:**

Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS:
(DisableIPSourceRouting) IP source routing protection level

Note: This Group Policy path does not exist by default. An additional Group Policy template (**MSS-legacy.admx/adml**) is required - it is available from this TechNet blog post: [The MSS settings – Microsoft Security Guidance blog](#)

Default Value:

Medium, source routed packets ignored when IP forwarding is enabled.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224917
Rule ID: SV-224917r569186_rule
STIG ID: WN16-CC-000050
Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

18.5.4 Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

Internet Control Message Protocol (ICMP) redirects cause the IPv4 stack to plumb host routes. These routes override the Open Shortest Path First (OSPF) generated routes.

The recommended state for this setting is: **Disabled**.

Rationale:

This behavior is expected. The problem is that the 10 minute time-out period for the ICMP redirect-plumbed routes temporarily creates a network situation in which traffic will no longer be routed properly for the affected host. Ignoring such ICMP redirects will limit the system's exposure to attacks that will impact its ability to participate on the network.

Impact:

When Routing and Remote Access Service (RRAS) is configured as an autonomous system boundary router (ASBR), it does not correctly import connected interface subnet routes. Instead, this router injects host routes into the OSPF routes. However, the OSPF router cannot be used as an ASBR router, and when connected interface subnet routes are imported into OSPF the result is confusing routing tables with strange routing paths.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters:EnableICMPRedirect

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS:
(EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes

Note: This Group Policy path does not exist by default. An additional Group Policy template (**MSS-legacy.admx/adml**) is required - it is available from this TechNet blog post: [The MSS settings – Microsoft Security Guidance blog](#)

Default Value:

Enabled. (ICMP redirects can override OSPF-generated routes.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224918
Rule ID: SV-224918r569186_rule
STIG ID: WN16-CC-000060
Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.			

18.5.5 Ensure 'MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds' is set to 'Enabled: 300,000 or 5 minutes' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This value controls how often TCP attempts to verify that an idle connection is still intact by sending a keep-alive packet. If the remote computer is still reachable, it acknowledges the keep-alive packet.

The recommended state for this setting is: **Enabled: 300,000 or 5 minutes.**

Rationale:

An attacker who is able to connect to network applications could establish numerous connections to cause a DoS condition.

Impact:

Keep-alive packets are not sent by default by Windows. However, some applications may configure the TCP stack flag that requests keep-alive packets. For such configurations, you can lower this value from the default setting of two hours to five minutes to disconnect inactive sessions more quickly.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **300000**.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters:KeepAliveTime
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled: 300,000 or 5 minutes**:

```
Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS:  
(KeepAliveTime) How often keep-alive packets are sent in milliseconds
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (**MSS-legacy.admx/adml**) is required - it is available from this TechNet blog post: [The MSS settings – Microsoft Security Guidance blog](#)

Default Value:

7,200,000 milliseconds or 120 minutes.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			

18.5.6 Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

NetBIOS over TCP/IP is a network protocol that among other things provides a way to easily resolve NetBIOS names that are registered on Windows-based systems to the IP addresses that are configured on those systems. This setting determines whether the computer releases its NetBIOS name when it receives a name-release request.

The recommended state for this setting is: **Enabled**.

Rationale:

The NetBT protocol is designed not to use authentication, and is therefore vulnerable to spoofing. Spoofing makes a transmission appear to come from a user other than the user who performed the action. A malicious user could exploit the unauthenticated nature of the protocol to send a name-conflict datagram to a target computer, which would cause the computer to relinquish its name and not respond to queries.

An attacker could send a request over the network and query a computer to release its NetBIOS name. As with any change that could affect applications, it is recommended that you test this change in a non-production environment before you change the production environment.

The result of such an attack could be to cause intermittent connectivity issues on the target computer, or even to prevent the use of Network Neighborhood, domain logons, the NET SEND command, or additional NetBIOS name resolution.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SYSTEM\CurrentControlSet\Services\NetBT\Parameters:NoNameReleaseOnDemand
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS:  
(NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release  
requests except from WINS servers
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (**MSS-legacy.admx/adml**) is required - it is available from this TechNet blog post: [The MSS settings – Microsoft Security Guidance blog](#)

Default Value:

Enabled.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224919
Rule ID: SV-224919r852324_rule
STIG ID: WN16-CC-000070
Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

18.5.7 Ensure 'MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This setting is used to enable or disable the Internet Router Discovery Protocol (IRDP), which allows the system to detect and configure default gateway addresses automatically as described in RFC 1256 on a per-interface basis.

The recommended state for this setting is: **Disabled**.

Rationale:

An attacker who has gained control of a computer on the same network segment could configure a computer on the network to impersonate a router. Other computers with IRDP enabled would then attempt to route their traffic through the already compromised computer.

Impact:

Windows will not automatically detect and configure default gateway addresses on the computer.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters:PerformRouterDiscovery
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS:  
(PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway  
addresses
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (**MSS-legacy.admx/adml**) is required - it is available from this TechNet blog post: [The MSS settings – Microsoft Security Guidance blog](#)

Default Value:

Enable only if DHCP sends the Perform Router Discovery option.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

18.5.8 Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

The DLL search order can be configured to search for DLLs that are requested by running processes in one of two ways:

- Search folders specified in the system path first, and then search the current working folder.
- Search current working folder first, and then search the folders specified in the system path.

When enabled, the registry value is set to 1. With a setting of 1, the system first searches the folders that are specified in the system path and then searches the current working folder. When disabled the registry value is set to 0 and the system first searches the current working folder and then searches the folders that are specified in the system path.

Applications will be forced to search for DLLs in the system path first. For applications that require unique versions of these DLLs that are included with the application, this entry could cause performance or stability problems.

The recommended state for this setting is: **Enabled**.

Note: More information on how Safe DLL search mode works is available at this link: [Dynamic-Link Library Search Order - Windows applications | Microsoft Docs](#)

Rationale:

If a user unknowingly executes hostile code that was packaged with additional files that include modified versions of system DLLs, the hostile code could load its own versions of those DLLs and potentially increase the type and degree of damage the code can render.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

HKLM\SYSTEM\CurrentControlSet\Control\Session Manager:SafeDllSearchMode

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (SafeDllSearchMode) Enable Safe DLL search mode

Note: This Group Policy path does not exist by default. An additional Group Policy template (**MSS-legacy.admx/adml**) is required - it is available from this TechNet blog post: [The MSS settings – Microsoft Security Guidance blog](#)

Default Value:

Enabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 <u>Enable Anti-Exploitation Features</u> Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 <u>Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies</u> Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

18.5.9 Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires' is set to 'Enabled: 5 or fewer seconds' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Windows includes a grace period between when the screen saver is launched and when the console is actually locked automatically when screen saver locking is enabled.

The recommended state for this setting is: **Enabled: 5 or fewer seconds**.

Rationale:

The default grace period that is allowed for user movement before the screen saver lock takes effect is five seconds. If you leave the default grace period configuration, your computer is vulnerable to a potential attack from someone who could approach the console and attempt to log on to the computer before the lock takes effect. An entry to the registry can be made to adjust the length of the grace period.

Impact:

Users will have to enter their passwords to resume their console sessions as soon as the grace period ends after screen saver activation.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_SZ** value of **5**.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\Winlogon:ScreenSaverGracePeriod
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled: 5 or fewer seconds**:

```
Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS:  
(ScreenSaverGracePeriod) The time in seconds before the screen saver grace  
period expires
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (**MSS-legacy.admx/adml**) is required - it is available from this TechNet blog post: [The MSS settings – Microsoft Security Guidance blog](#)

Default Value:

5 seconds.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.3 Configure Automatic Session Locking on Enterprise Assets</u> Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.			
v7	<u>16.11 Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity.			

18.5.10 Ensure 'MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This setting controls the number of times that TCP retransmits an individual data segment (non-connect segment) before the connection is aborted. The retransmission time-out is doubled with each successive retransmission on a connection. It is reset when responses resume. The base time-out value is dynamically determined by the measured round-trip time on the connection.

The recommended state for this setting is: **Enabled: 3**.

Rationale:

A malicious user could exhaust a target computer's resources if it never sent any acknowledgment messages for data that was transmitted by the target computer.

Impact:

TCP starts a retransmission timer when each outbound segment is passed to the IP. If no acknowledgment is received for the data in a given segment before the timer expires, then the segment is retransmitted up to three times.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **3**.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TCPIP6\Parameters:TcpMaxDataRetransmissions
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled: 3**:

```
Computer Configuration\Policies\Administrative Templates\MSS  
(Legacy)\MSS:(TcpMaxDataRetransmissions IPv6) How many times unacknowledged  
data is retransmitted
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (**MSS-legacy.admx/adml**) is required - it is available from this TechNet blog post: [The MSS settings – Microsoft Security Guidance blog](#)

Default Value:

5 times.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure</u> Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	<u>11.1 Maintain Standard Security Configurations for Network Devices</u> Maintain standard, documented security configuration standards for all authorized network devices.			

18.5.11 Ensure 'MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This setting controls the number of times that TCP retransmits an individual data segment (non-connect segment) before the connection is aborted. The retransmission time-out is doubled with each successive retransmission on a connection. It is reset when responses resume. The base time-out value is dynamically determined by the measured round-trip time on the connection.

The recommended state for this setting is: **Enabled: 3**.

Rationale:

A malicious user could exhaust a target computer's resources if it never sent any acknowledgment messages for data that was transmitted by the target computer.

Impact:

TCP starts a retransmission timer when each outbound segment is passed to the IP. If no acknowledgment is received for the data in a given segment before the timer expires, then the segment is retransmitted up to three times.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **3**.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters:TcpMaxDataRetransmissions
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled: 3**:

```
Computer Configuration\Policies\Administrative Templates\MSS  
(Legacy)\MSS:(TcpMaxDataRetransmissions) How many times unacknowledged data  
is retransmitted
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (**MSS-legacy.admx/adml**) is required - it is available from this TechNet blog post: [The MSS settings – Microsoft Security Guidance blog](#)

Default Value:

5 times.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.2 <u>Establish and Maintain a Secure Configuration Process for Network Infrastructure</u> Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

18.5.12 Ensure 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' is set to 'Enabled: 90% or less' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This setting can generate a security audit in the Security event log when the log reaches a user-defined threshold.

The recommended state for this setting is: **Enabled: 90% or less**.

Note: If log settings are configured to Overwrite events as needed or Overwrite events older than x days, this event will not be generated.

Rationale:

If the Security log reaches 90 percent of its capacity and the computer has not been configured to overwrite events as needed, more recent events will not be written to the log. If the log reaches its capacity and the computer has been configured to shut down when it can no longer record events to the Security log, the computer will shut down and will no longer be available to provide network services.

Impact:

An audit event will be generated when the Security log reaches the 90% percent full threshold (or whatever lower value may be set) unless the log is configured to overwrite events as needed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **90**.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security:WarningLevel
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled: 90% or less**:

Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning

Note: This Group Policy path does not exist by default. An additional Group Policy template (**MSS-legacy.admx/adml**) is required - it is available from this TechNet blog post: [The MSS settings – Microsoft Security Guidance blog](#)

Default Value:

0%. (No warning event is generated.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 <u>Ensure Adequate Audit Log Storage</u> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.			
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			
v7	6.4 <u>Ensure adequate storage for logs</u> Ensure that all systems that store logs have adequate storage space for the logs generated.			

18.6 Network

This section contains recommendations for network settings.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.6.1 Background Intelligent Transfer Service (BITS)

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Bits.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.6.2 BranchCache

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `PeerToPeerCaching.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.6.3 DirectAccess Client Experience Settings

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `nca.admx/adml` that is included with the Microsoft 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.6.4 DNS Client

This section contains recommendations related to DNS Client.

This Group Policy section is provided by the Group Policy template `DnsClient.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.6.4.1 Ensure 'Configure NetBIOS settings' is set to 'Enabled: Disable NetBIOS name resolution on public networks' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting specifies if the Domain Name System (DNS) client will perform name resolution over Network Basic Input/Output System (NetBIOS). NetBIOS is a legacy name resolution method for internal Microsoft networking that predates the use of DNS for that purpose (pre-Active Directory). Some legacy applications still require the use of NetBIOS for full functionality.

The recommended state for this setting is: **Enabled: Disable NetBIOS name resolution on public networks**. Configuring this setting to **Enabled: Disable NetBIOS name resolution** also conforms to the benchmark.

Rationale:

NetBIOS does not perform authentication and can allow remote attackers to cause a denial of service by sending spoofed Name Conflicts or Name Release datagrams. This is also known as "NetBIOS Name Server Protocol Spoofing". Preventing the use of NetBIOS on public networks reduces the attack surface.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0** or **2**.

HKLM\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient:EnableNetbios

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled: Disable NetBIOS name resolution on public networks:**

```
Computer Configuration\Policies\Administrative Templates\Network\DNS
Client\Configure NetBIOS settings
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **DnsClient.admx/adml** that is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v1.0 (or newer).

Default Value:

Enabled. (The DNS client will disable NetBIOS name resolution on public networks.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			

18.6.4.2 Ensure 'Turn off multicast name resolution' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Member Server
- Level 1 - Domain Controller

Description:

LLMNR is a secondary name resolution protocol. With LLMNR, queries are sent using multicast over a local network link on a single subnet from a client computer to another client computer on the same subnet that also has LLMNR enabled. LLMNR does not require a DNS server or DNS client configuration, and provides name resolution in scenarios in which conventional DNS name resolution is not possible.

The recommended state for this setting is: **Enabled**.

Rationale:

An attacker can listen on a network for these LLMNR (UDP/5355) or NBT-NS (UDP/137) broadcasts and respond to them, tricking the host into thinking that it knows the location of the requested system.

Note: To completely mitigate local name resolution poisoning, in addition to this setting, the properties of each installed NIC should also be set to **Disable NetBIOS over TCP/IP** (on the WINS tab in the NIC properties). Unfortunately, there is no global setting to achieve this that automatically applies to all NICs - it is a per-NIC setting that varies with different NIC hardware installations.

Impact:

In the event DNS is unavailable a system will be unable to request it from other systems on the same subnet.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

HKLM\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient:EnableMulticast

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

Computer Configuration\Policies\Administrative Templates\Network\DNS
Client\Turn off multicast name resolution

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **DnsClient.admx/adml** that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (LLMNR will be enabled on all available network adapters.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

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).

18.6.5.1 Ensure 'Enable Font Providers' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting determines whether Windows is allowed to download fonts and font catalog data from an online font provider.

The recommended state for this setting is: **Disabled**.

Rationale:

In an enterprise managed environment the IT department should be managing the changes to the system configuration, to ensure all changes are tested and approved.

Impact:

Windows will not connect to an online font provider and will only enumerate locally-installed fonts.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\System:EnableFontProviders
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Administrative Templates\Network\Fonts\Enable Font Providers
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **GroupPolicy.admx/adml** that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

Default Value:

Enabled. (Fonts that are included in Windows but that are not stored locally will be downloaded on demand from an online font provider.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>16.5 Use Up-to-Date and Trusted Third-Party Software Components</u> Use up-to-date and trusted third-party software components. When possible, choose established and proven frameworks and libraries that provide adequate security. Acquire these components from trusted sources or evaluate the software for vulnerabilities before use.		●	●
v7	<u>18.4 Only Use Up-to-date And Trusted Third-Party Components</u> Only use up-to-date and trusted third-party components for the software developed by the organization.		●	●

18.6.6 Hotspot Authentication

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template [hotspotauth.admx/adml](#) that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.6.7 Lanman Server

This section is 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).

18.6.8.1 Ensure 'Enable insecure guest logons' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting determines if the SMB client will allow insecure guest logons to an SMB server.

The recommended state for this setting is: **Disabled**.

Rationale:

Insecure guest logons are used by file servers to allow unauthenticated access to shared folders.

Impact:

The SMB client will reject insecure guest logons. This was not originally the default behavior in older versions of Windows, but Microsoft changed the default behavior starting with Windows Server 2016 R1709: [Guest access in SMB2 disabled by default in Windows 10 and Windows Server 2016](#)

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\LanmanWorkstation:AllowInsecureGuestAuth
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Administrative Templates\Network\Lanman Workstation\Enable insecure guest logons
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **LanmanWorkstation.admx/adml** that is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).

Default Value:

Server 2016 RTM (R1607) or older: Enabled. (The SMB client will allow insecure guest logons.)

Server 2016 R1709, Server 2019 or newer: Disabled. (The SMB client will reject insecure guest logons.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224920
Rule ID: SV-224920r569186_rule
STIG ID: WN16-CC-000080
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

18.6.9 Link-Layer Topology Discovery

This section contains recommendations for Link-Layer Topology Discovery settings.

This Group Policy section is provided by the Group Policy template [LinkLayerTopologyDiscovery.admx/adml](#) that is included with all versions of the Microsoft Windows Administrative Templates.

18.6.9.1 Ensure 'Turn on Mapper I/O (LLTDIO) driver' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting changes the operational behavior of the Mapper I/O network protocol driver.

LLTDIO allows a computer to discover the topology of a network it's connected to. It also allows a computer to initiate Quality-of-Service requests such as bandwidth estimation and network health analysis.

The recommended state for this setting is: **Disabled**.

Rationale:

To help protect from potentially discovering and connecting to unauthorized devices, this setting should be disabled to prevent responding to network traffic for network topology discovery.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry locations with a **REG_DWORD** value of **0**.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\LLTD:AllowLLTDIOOnDomain
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\LLTD:AllowLLTDIOOnPublicNet
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\LLTD:EnableLLTDIO
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\LLTD:ProhibitLLTDIOOnPrivateNet
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

Computer Configuration\Policies\Administrative Templates\Network\Link-Layer Topology Discovery\Turn on Mapper I/O (LLTDIO) driver

Note: This Group Policy path is provided by the Group Policy template **LinkLayerTopologyDiscovery.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (The Mapper I/O (LLTDIO) network protocol driver is turned off.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

18.6.9.2 Ensure 'Turn on Responder (RSPNDR) driver' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting changes the operational behavior of the Responder network protocol driver.

The Responder allows a computer to participate in Link Layer Topology Discovery requests so that it can be discovered and located on the network. It also allows a computer to participate in Quality-of-Service activities such as bandwidth estimation and network health analysis.

The recommended state for this setting is: **Disabled**.

Rationale:

To help protect from potentially discovering and connecting to unauthorized devices, this setting should be disabled to prevent responding to network traffic for network topology discovery.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry locations with a **REG_DWORD** value of **0**.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\LLTD:AllowRspndrOnDomain
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\LLTD:AllowRspndrOnPublicNet
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\LLTD:EnableRspndr
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\LLTD:ProhibitRspndrOnPrivateNet
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

Computer Configuration\Policies\Administrative Templates\Network\Link-Layer Topology Discovery\Turn on Responder (RSPNDR) driver

Note: This Group Policy path is provided by the Group Policy template **LinkLayerTopologyDiscovery.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (The Responder (RSPNDR) network protocol driver is turned off.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

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-pnnp.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-pnnp.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

18.6.10.2 Ensure 'Turn off Microsoft Peer-to-Peer Networking Services' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

The Peer Name Resolution Protocol (PNRP) allows for distributed resolution of a name to an IPv6 address and port number. The protocol operates in the context of *clouds*. A cloud is a set of peer computers that can communicate with each other by using the same IPv6 scope.

Peer-to-Peer protocols allow for applications in the areas of RTC, collaboration, content distribution and distributed processing.

The recommended state for this setting is: **Enabled**.

Rationale:

This setting enhances the security of the environment and reduces the overall risk exposure related to peer-to-peer networking.

Impact:

Microsoft Peer-to-Peer Networking Services are turned off in their entirety, and all applications dependent on them will stop working.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Peernet:Disabled
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\Network\Microsoft  
Peer-to-Peer Networking Services\Turn off Microsoft Peer-to-Peer Networking  
Services
```

Note: This Group Policy path is provided by the Group Policy template **P2P-pnnp.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Peer-to-peer protocols are turned on.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

18.6.11 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.

18.6.11.2 Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

You can use this procedure to control a user's ability to install and configure a Network Bridge.

The recommended state for this setting is: **Enabled**.

Rationale:

The Network Bridge setting, if enabled, allows users to create a Layer 2 Media Access Control (MAC) bridge, enabling them to connect two or more physical network segments together. A Network Bridge thus allows a computer that has connections to two different networks to share data between those networks.

In an enterprise managed environment, where there is a need to control network traffic to only authorized paths, allowing users to create a Network Bridge increases the risk and attack surface from the bridged network.

Impact:

Users cannot create or configure a Network Bridge.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Network  
Connections:NC_AllowNetBridge_NLA
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

Computer Configuration\Policies\Administrative Templates\Network\Network Connections\Prohibit installation and configuration of Network Bridge on your DNS domain network

Note: This Group Policy path is provided by the Group Policy template **NetworkConnections.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Users are able create and modify the configuration of Network Bridges. Membership in the local Administrators group, or equivalent, is the minimum required to complete this procedure.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure</u> Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	<u>11.3 Use Automated Tools to Verify Standard Device Configurations and Detect Changes</u> Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.			

18.6.11.3 Ensure 'Prohibit use of Internet Connection Sharing on your DNS domain network' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Although this "legacy" setting traditionally applied to the use of Internet Connection Sharing (ICS) in Windows 2000, Windows XP & Server 2003, this setting now freshly applies to the Mobile Hotspot feature in Windows 10 & Server 2016.

The recommended state for this setting is: **Enabled**.

Rationale:

Non-administrators should not be able to turn on the Mobile Hotspot feature and open their Internet connectivity up to nearby mobile devices.

Impact:

Mobile Hotspot cannot be enabled or configured by Administrators and non-Administrators alike.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Network  
Connections:NC_ShowSharedAccessUI
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\Network\Network  
Connections\Prohibit use of Internet Connection Sharing on your DNS domain  
network
```

Note: This Group Policy path is provided by the Group Policy template **NetworkConnections.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (All users are allowed to turn on Mobile Hotspot.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

18.6.11.4 Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether to require domain users to elevate when setting a network's location.

The recommended state for this setting is: **Enabled**.

Rationale:

Allowing regular users to set a network location increases the risk and attack surface.

Impact:

Domain users must elevate when setting a network's location.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Network  
Connections\NC_StdDomainUserSetLocation
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\Network\Network  
Connections\Require domain users to elevate when setting a network's location
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **NetworkConnections.admx/adml** that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

Disabled. (Users can set a network's location without elevating.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

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).

18.6.14.1 Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication", "Require Integrity", and "Require Privacy" set for all NETLOGON and SYSVOL shares' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting configures secure access to UNC paths.

The recommended state for this setting is: **Enabled, with "Require Mutual Authentication", "Require Integrity", and "Require Privacy" set for all NETLOGON and SYSVOL shares.**

Rationale:

In February 2015, Microsoft released a new control mechanism to mitigate a security risk in Group Policy as part of the [MS15-011](#) / [MSKB 3000483](#) security update. This mechanism requires both the installation of the new security update and also the deployment of specific group policy settings to all computers on the domain from Windows Vista / Server 2008 (non-R2) or newer (the associated security patch to enable this feature was not released for Server 2003). A new group policy template (**NetworkProvider.admx/adml**) was also provided with the security update.

Once the new GPO template is in place, the following are the minimum requirements to remediate the Group Policy security risk:

```
\\*\NETLOGON RequireMutualAuthentication=1, RequireIntegrity=1,
RequirePrivacy=1
\\*\SYSVOL RequireMutualAuthentication=1, RequireIntegrity=1,
RequirePrivacy=1
```

Note: A reboot may be required after the setting is applied to a client machine to access the above paths.

Additional guidance on the deployment of this security setting is available from the Microsoft Premier Field Engineering (PFE) Platforms TechNet Blog here: [Guidance on Deployment of MS15-011 and MS15-014](#).

Impact:

Windows only allows access to the specified UNC paths after fulfilling additional security requirements.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry locations with a REG_SZ value of **RequireMutualAuthentication=1, RequireIntegrity=1, RequirePrivacy=1**.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths:\\*\NETLOGON
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths:\\*\SYSVOL
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled** with the following paths configured, at a minimum:

***\NETLOGON RequireMutualAuthentication=1, RequireIntegrity=1, RequirePrivacy=1**
***\SYSVOL RequireMutualAuthentication=1, RequireIntegrity=1, RequirePrivacy=1**

```
Computer Configuration\Policies\Administrative Templates\Network\Network Provider\Hardened UNC Paths
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (**NetworkProvider.admx/adml**) is required - it is included with the [MS15-011](#) / [MSKB 3000483](#) security update or with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

Default Value:

Disabled. (No UNC paths are hardened.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

18.6.14.2 Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication", "Require Integrity" set for all NETLOGON and SYSVOL shares' (STIG only) (Automated)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting configures secure access to UNC paths.

The recommended state for this setting is: **Enabled, with "Require Mutual Authentication", "Require Integrity", and "Require Privacy" set for all NETLOGON and SYSVOL shares.**

Rationale:

In February 2015, Microsoft released a new control mechanism to mitigate a security risk in Group Policy as part of the [MS15-011](#) / [MSKB 3000483](#) security update. This mechanism requires both the installation of the new security update and also the deployment of specific group policy settings to all computers on the domain from Windows Vista / Server 2008 (non-R2) or newer (the associated security patch to enable this feature was not released for Server 2003). A new group policy template ([NetworkProvider.admx/adml](#)) was also provided with the security update.

Once the new GPO template is in place, the following are the minimum requirements to remediate the Group Policy security risk:

***\NETLOGON RequireMutualAuthentication=1, RequireIntegrity=1 =1**

***\SYSVOL RequireMutualAuthentication=1, RequireIntegrity=1 =1**

Note: A reboot may be required after the setting is applied to a client machine to access the above paths.

Additional guidance on the deployment of this security setting is available from the Microsoft Premier Field Engineering (PFE) Platforms TechNet Blog here: [Guidance on Deployment of MS15-011 and MS15-014](#).

Impact:

Windows only allows access to the specified UNC paths after fulfilling additional security requirements.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry locations with a **REG_SZ** value of **RequireMutualAuthentication=1, RequireIntegrity=1, RequirePrivacy=1**.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths:\\*\NETLOGON
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths:\\*\SYSVOL
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled** with the following paths configured, at a minimum:

***\NETLOGON RequireMutualAuthentication=1, RequireIntegrity=1**
***\SYSVOL RequireMutualAuthentication=1, RequireIntegrity=1**

```
Computer Configuration\Policies\Administrative Templates\Network\Network Provider\Hardened UNC Paths
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (**NetworkProvider.admx/adml**) is required - it is included with the [MS15-011](#) / [MSKB 3000483](#) security update or with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

Default Value:

Disabled. (No UNC paths are hardened.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide: Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224921 Rule ID: SV-224921r857251_rule STIG ID: WN16-CC-000090
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

18.6.15 Offline Files

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template **OfflineFiles.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

18.6.16 QoS Packet Scheduler

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template **QOS.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

18.6.17 SNMP

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template **Snmp.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

18.6.18 SSL Configuration Settings

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template **CipherSuiteOrder.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

18.6.19 TCPIP Settings

This section contains TCP/IP configuration settings.

This Group Policy section is provided by the Group Policy template `tcpip.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.6.19.1 IPv6 Transition Technologies

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `tcpip.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.6.19.2 Parameters

This section contains TCP/IP parameter configuration settings.

This Group Policy section is provided by the Group Policy template `tcpip.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.6.19.2.1 Disable IPv6 (Ensure TCPIP6 Parameter 'DisabledComponents' is set to '0xff (255)') (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

Internet Protocol version 6 (IPv6) is a set of protocols that computers use to exchange information over the Internet and over home and business networks. IPv6 allows for many more IP addresses to be assigned than IPv4 did. Older networking, hosts and operating systems may not support IPv6 natively.

The recommended state for this setting is: **DisabledComponents - 0xff (255)**

Rationale:

Since the vast majority of private enterprise managed networks have no need to utilize IPv6 (because they have access to private IPv4 addressing), disabling IPv6 components removes a possible attack surface that is also harder to monitor the traffic on. As a result, we recommend configuring IPv6 to a Disabled state when it is not needed.

Impact:

Connectivity to other systems using IPv6 will no longer operate, and software that depends on IPv6 will cease to function. Examples of Microsoft applications that may use IPv6 include: Remote Assistance, HomeGroup, DirectAccess, Windows Mail.

This registry change is documented in Microsoft Knowledge Base article 929852: [How to disable IPv6 or its components in Windows](#).

Note: This registry change does not take effect until the next reboot.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **255**.

HKLM\SYSTEM\CurrentControlSet\Services\TCPIP6\Parameters:DisabledComponents

Remediation:

To establish the recommended configuration, set the following Registry value to **0xff (255) (DWORD)**:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TCPIP6\Parameters:DisabledComponents

Note: This change does not take effect until the computer has been restarted.

Note #2: Although Microsoft does not provide an ADMX template to configure this registry value, a custom .ADM template (**Disable-IPv6-Components-KB929852.adm**) is provided in the CIS Benchmark Remediation Kit to facilitate its configuration. Be aware though that simply turning off the group policy setting in the .ADM template will not "undo" the change once applied. Instead, the opposite setting must be applied to change the registry value to the opposite state.

Default Value:

All IPv6 components are enabled and Windows prefers IPv6 over IPv4.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

18.6.20 Windows Connect Now

This section contains recommendations for Windows Connect Now settings.

This Group Policy section is provided by the Group Policy template [WindowsConnectNow.admx/adml](#) that is included with all versions of the Microsoft Windows Administrative Templates.

18.6.20.1 Ensure 'Configuration of wireless settings using Windows Connect Now' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting allows the configuration of wireless settings using Windows Connect Now (WCN). The WCN Registrar enables the discovery and configuration of devices over Ethernet (UPnP) over in-band 802.11 Wi-Fi through the Windows Portable Device API (WPD) and via USB Flash drives. Additional options are available to allow discovery and configuration over a specific medium.

The recommended state for this setting is: **Disabled**.

Rationale:

This setting enhances the security of the environment and reduces the overall risk exposure related to user configuration of wireless settings.

Impact:

WCN operations are disabled over all media.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry locations with a **REG_DWORD** value of **0**.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WCN\Registrars:EnableR  
egistrars  
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WCN\Registrars:Disable  
UPnPRegistrar  
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WCN\Registrars:Disable  
InBand802DOT11Registrar  
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WCN\Registrars:Disable  
FlashConfigRegistrar  
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WCN\Registrars:Disable  
WPDRegistrar
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

Computer Configuration\Policies\Administrative Templates\Network\Windows Connect Now\Configuration of wireless settings using Windows Connect Now

Note: This Group Policy path is provided by the Group Policy template **WindowsConnectNow.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

WCN operations are enabled and allowed over all media.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	15.4 <u>Disable Wireless Access on Devices if Not Required</u> Disable wireless access on devices that do not have a business purpose for wireless access.			●
v7	15.5 <u>Limit Wireless Access on Client Devices</u> Configure wireless access on client machines that do have an essential wireless business purpose, to allow access only to authorized wireless networks and to restrict access to other wireless networks.			●

18.6.20.2 Ensure 'Prohibit access of the Windows Connect Now wizards' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting prohibits access to Windows Connect Now (WCN) wizards.

The recommended state for this setting is: **Enabled**.

Rationale:

Allowing standard users to access the Windows Connect Now wizard increases the risk and attack surface.

Impact:

The WCN wizards are turned off and users have no access to any of the wizard tasks. All the configuration related tasks including "Set up a wireless router or access point" and "Add a wireless device" are disabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\WCN\UI:DisableWcnUi
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\Network\Windows  
Connect Now\Prohibit access of the Windows Connect Now wizards
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **WindowsConnectNow.admx/adml** that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (Users can access all WCN wizard tasks.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

18.6.21 Windows Connection Manager

This section contains recommendations for Windows Connection Manager settings.

This Group Policy section is provided by the Group Policy template `WCM.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.6.21.1 Ensure 'Minimize the number of simultaneous connections to the Internet or a Windows Domain' is set to 'Enabled: 1 = Minimize simultaneous connections' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting prevents computers from establishing multiple simultaneous connections to either the Internet or to a Windows domain.

The recommended state for this setting is: **Enabled: 1 = Minimize simultaneous connections**.

Rationale:

Preventing bridged network connections can help prevent a user unknowingly allowing traffic to route between internal and external networks, which risks exposure to sensitive internal data.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\WcmSvc\GroupPolicy:fMinimizeConnections
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled: 1 = Minimize simultaneous connections**:

```
Computer Configuration\Policies\Administrative Templates\Network\Windows Connection Manager\Minimize the number of simultaneous connections to the Internet or a Windows Domain
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **WCM.admx/adml** that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates. It was updated with a new *Minimize Policy Options* sub-setting starting with the Windows 10 Release 1903 Administrative Templates.

Default Value:

Enabled: 1 = Minimize simultaneous connections. (Any new automatic internet connection is blocked when the computer has at least one active internet connection to a preferred type of network. The order of preference (from most preferred to least preferred) is: Ethernet, WLAN, then cellular. Ethernet is always preferred when connected. Users can still manually connect to any network.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	15.5 <u>Limit Wireless Access on Client Devices</u> Configure wireless access on client machines that do have an essential wireless business purpose, to allow access only to authorized wireless networks and to restrict access to other wireless networks.			

18.6.21.2 Ensure 'Prohibit connection to non-domain networks when connected to domain authenticated network' is set to 'Enabled' (MS only) (Automated)

Profile Applicability:

- Level 2 - Member Server

Description:

This policy setting prevents computers from connecting to both a domain based network and a non-domain based network at the same time.

The recommended state for this setting is: **Enabled**.

Rationale:

The potential concern is that a user would unknowingly allow network traffic to flow between the insecure public network and the enterprise managed network.

Impact:

The computer responds to automatic and manual network connection attempts based on the following circumstances:

Automatic connection attempts - When the computer is already connected to a domain based network, all automatic connection attempts to non-domain networks are blocked.
- When the computer is already connected to a non-domain based network, automatic connection attempts to domain based networks are blocked.

Manual connection attempts - When the computer is already connected to either a non-domain based network or a domain based network over media other than Ethernet, and a user attempts to create a manual connection to an additional network in violation of this policy setting, the existing network connection is disconnected and the manual connection is allowed. - When the computer is already connected to either a non-domain based network or a domain based network over Ethernet, and a user attempts to create a manual connection to an additional network in violation of this policy setting, the existing Ethernet connection is maintained and the manual connection attempt is blocked.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\WcmSvc\GroupPolicy:fBlockNonDomain
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\Network\Windows  
Connection Manager\Prohibit connection to non-domain networks when connected  
to domain authenticated network
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **WCM.admx/adm1** that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (Connections to both domain and non-domain networks are simultaneously allowed.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	12.4 <u>Deny Communication over Unauthorized Ports</u> Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.			

18.7 Printers

This section contains recommendations for printer settings.

This Group Policy section is provided by the Group Policy template [Printing.admx/adml](#) that is included with all versions of the Microsoft Windows Administrative Templates.

18.7.1 Ensure 'Allow Print Spooler to accept client connections' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting controls whether the Print Spooler service will accept client connections.

The recommended state for this setting is: **Disabled**.

Note: The Print Spooler service must be restarted for changes to this policy to take effect.

Warning: An exception to this recommendation must be made for print servers in order for them to function properly. Users will not be able to print to the server when client connections are disabled.

Rationale:

Disabling the ability for the Print Spooler service to accept client connections mitigates **remote** attacks against the PrintNightmare vulnerability ([CVE-2021-34527](#)) and other **remote** Print Spooler attacks. However, this recommendation *does not* mitigate against **local** attacks on the Print Spooler service.

Impact:

Provided that the Print Spooler service is not disabled, applications on and users logged in to servers will continue to be able to print *from the server*. However, the Print Spooler service will not accept client connections or allow users to share printers. Note that all printers that were already shared will continue to be shared.

Warning: An exception to this recommendation must be made for print servers in order for them to function properly. Users will not be able to print to the server when client connections are disabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **2**.

```
HKLM\Software\Policies\Microsoft\Windows  
NT\Printers:RegisterSpoolerRemoteRpcEndPoint
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Administrative Templates\Printers:Allow Print  
Spooler to accept client connections
```

Note: This Group Policy path is provided by the Group Policy template **Printing2.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Enabled. (The Print Spooler will always accept client connections.)

References:

1. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			

18.7.2 Ensure 'Configure Redirection Guard' is set to 'Enabled: Redirection Guard Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether Redirection Guard is enabled for the print spooler. Redirection Guard can prevent file redirections from being used within the print spooler.

The recommended state for this setting is: **Enabled: Redirection Guard Enabled**.

Rationale:

This setting prevents non-administrators from redirecting files within the print spooler process.

Impact:

None - this is default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Printers:RedirectionguardPolicy
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled: Redirection Guard Enabled**:

```
Computer Configuration\Policies\Administrative Templates\Printers\Configure Redirection Guard
```

Note: This Group Policy path is provided by the Group Policy template **Printing.admx/adml** that is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v1.0 (or newer).

Default Value:

Disabled. (Redirection Guard will default to being "Enabled".)

References:

1. <https://techcommunity.microsoft.com/t5/microsoft-security-baselines/windows-11-version-22h2-security-baseline/ba-p/3632520>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 <u>Enable Anti-Exploitation Features</u> Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●

18.7.3 Ensure 'Configure RPC connection settings: Protocol to use for outgoing RPC connections' is set to 'Enabled: RPC over TCP' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls which protocol and protocol settings to use for outgoing Remote Procedure Call (RPC) connections to a remote print spooler.

The recommended state for this setting is: **Enabled: RPC over TCP**

Rationale:

This setting prevents the use of named pipes for RPC connections to the print spooler and forces the use of TCP which is a more secure communication method.

Impact:

Warning: Many existing print configurations may be using the older named pipes protocol and therefore will cease to function.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows  
NT\Printers\RPC:RpcUseNamedPipeProtocol
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled: RPC over TCP**:

```
Computer Configuration\Policies\Administrative Templates\Printers\Configure  
RPC connection settings: Protocol to use for outgoing RPC connections
```

Note: This Group Policy path is provided by the Group Policy template **Printing.admx/adml** that is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v1.0 (or newer).

Default Value:

Disabled. (By default, RPC over TCP is used. For RPC over named pipes, authentication is always enabled for domain joined machines but disabled for non-domain joined machines.)

References:

1. <https://learn.microsoft.com/en-us/troubleshoot/windows-client/printing/windows-11-rpc-connection-updates-for-print#allow-rpc-over-tcp-communication>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

18.7.4 Ensure 'Configure RPC connection settings: Use authentication for outgoing RPC connections' is set to 'Enabled: Default' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls which protocol and protocol settings to use for outgoing Remote Procedure Call (RPC) connections to a remote print spooler.

The recommended state for this setting is: **Enabled: Default**

Rationale:

This setting can prevent the use of named pipes for RPC connections to the print spooler and forces the use of TCP which is a more secure communication method.

Impact:

Warning: Many existing print configurations may be using the older named pipes protocol and therefore will cease to function.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Printers\RPC:RpcAuthentication
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled: Default**:

```
Computer Configuration\Policies\Administrative Templates\Printers\Configure  
RPC connection settings: Use authentication for outgoing RPC connections
```

Note: This Group Policy path is provided by the Group Policy template **Printing.admx/adml** that is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v1.0 (or newer).

Default Value:

Disabled. (By default, RPC over TCP is used. For RPC over named pipes, authentication is always enabled for domain joined machines but disabled for non-domain joined machines.)

References:

1. <https://learn.microsoft.com/en-us/troubleshoot/windows-client/printing/windows-11-rpc-connection-updates-for-print#allow-rpc-over-tcp-communication>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

18.7.5 Ensure 'Configure RPC listener settings: Protocols to allow for incoming RPC connections' is set to 'Enabled: RPC over TCP' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls which protocols incoming Remote Procedure Call (RPC) connections to the print spooler are allowed to use.

The recommended state for this setting is: **Enabled: RPC over TCP**.

Rationale:

This setting can prevent the use of named pipes for RPC connections to the print spooler and forces the use of TCP which is a more secure communication method.

Impact:

Warning: Many existing print configurations may be using the older named pipes protocol and therefore will cease to function.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **5**.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows  
NT\Printers\RPC:RpcProtocols
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled: RCP over TCP**:

```
Computer Configuration\Policies\Administrative Templates\Printers\Configure  
RPC listener settings: Configure protocol options for incoming RPC  
connections
```

Note: This Group Policy path is provided by the Group Policy template **Printing.admx/adml** that is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v1.0 (or newer).

Default Value:

Enabled. (RPC over TCP is enabled and Negotiate is used for the authentication protocol.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

18.7.6 Ensure 'Configure RPC listener settings: Authentication protocol to use for incoming RPC connections:' is set to 'Enabled: Negotiate' or higher (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls which protocols incoming Remote Procedure Call (RPC) connections to the print spooler are allowed to use.

The recommended state for this setting is: **Enabled: Negotiate** or higher.

Rationale:

This setting can prevent the use of named pipes for RPC connections to the print spooler and forces the use of TCP which is a more secure communication method.

Impact:

Warning: Many existing print configurations may be using the older named pipes protocol and therefore will cease to function.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0** or **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Printers\RPC:ForceKerberosForRpc
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled: Negotiate** or higher:

```
Computer Configuration\Policies\Administrative Templates\Printers\Configure  
RPC listener settings: Configure protocol options for incoming RPC  
connections
```

Note: This Group Policy path is provided by the Group Policy template **Printing.admx/adml** that is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v1.0 (or newer).

Default Value:

Enabled. (RPC over TCP is enabled and Negotiate is used for the authentication protocol.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

18.7.7 Ensure 'Configure RPC over TCP port' is set to 'Enabled: 0' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls which port is used for RPC over TCP for incoming connections to the print spooler and outgoing connections to remote print spoolers.

The recommended state for this setting is: **Enabled: 0**.

Rationale:

Using dynamic ports for printing makes it more difficult for an attacker to know which port is being used and therefore which port to attack.

Impact:

If your current print environment is configured for a specific TCP port, this setting may require a firewall change (if applicable) for continued printing.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Printers\RPC:RpcTcpPort
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled: 0**:

```
Computer Configuration\Policies\Administrative Templates\Printers\Configure  
RPC over TCP port
```

Note: This Group Policy path is provided by the Group Policy template **Printing.admx/adml** that is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v1.0 (or newer).

Default Value:

Disabled. (Dynamic TCP ports are used)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

18.7.8 Ensure 'Limits print driver installation to Administrators' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls whether users who aren't Administrators can install print drivers on the system.

The recommended state for this setting is: **Enabled**.

Note: On August 10, 2021, Microsoft announced a [Point and Print Default Behavior Change](#) which modifies the default Point and Print driver installation and update behavior to require Administrator privileges. This is documented in [KB5005652—Manage new Point and Print default driver installation behavior \(CVE-2021-34481\)](#).

Rationale:

Restricting the installation of print drives to Administrators can help mitigate the PrintNightmare vulnerability ([CVE-2021-34527](#)) and other Print Spooler attacks.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows  
NT\Printers\PointAndPrint:RestrictDriverInstallationToAdministrators
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**.

```
Computer Configuration\Policies\Administrative Templates\Printers\Limits  
print driver installation to Administrators
```

Note: This Group Policy path is provided by the Group Policy template **Printing.admx/adml** that is included with the Microsoft Windows 10 Release 21H2 Administrative Templates (or newer).

Default Value:

Enabled. (The system will limit installation of print drivers to Administrators of the computer.)

References:

1. <https://support.microsoft.com/en-us/topic/kb5005010-restricting-installation-of-new-printer-drivers-after-applying-the-july-6-2021-updates-31b91c02-05bc-4ada-a7ea-183b129578a7>
2. <https://support.microsoft.com/en-gb/topic/kb5005652-manage-new-point-and-print-default-driver-installation-behavior-cve-2021-34481-873642bf-2634-49c5-a23b-6d8e9a302872>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

18.7.9 Ensure 'Manage processing of Queue-specific files' is set to 'Enabled: Limit Queue-specific files to Color profiles' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting manages how queue-specific files are processed during printer installation. At printer installation time, a vendor-supplied installation application can specify a set of files, of any type, to be associated with a particular print queue. The files are downloaded to each client that connects to the print server.

The recommended state for this setting is: **Enabled: Limit Queue-specific files to Color profiles.**

Rationale:

A Windows Print Spooler Remote Code Execution Vulnerability ([CVE-2021-36958](#)) exists when the Windows Print Spooler service improperly performs privileged file operations. An attacker who successfully exploits this vulnerability could run arbitrary code with SYSTEM privileges and then install programs; view, change, or delete data; or create new accounts with full user rights.

Impact:

None - this is default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Printers:CopyFilesPolicy

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled: Limit Queue-specific files to Color profiles**:

Computer Configuration\Policies\Administrative Templates\Printers\Manage processing of Queue-specific files

Note: This Group Policy path is provided by the Group Policy template **Printing.admx/adml** that is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v1.0 (or newer).

Default Value:

Disabled. (Queue-specific files will be limited to Color profiles.)

References:

1. <https://learn.microsoft.com/en-us/windows-hardware/drivers/print/installing-queue-specific-files>
2. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36958>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 <u>Enable Anti-Exploitation Features</u> Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●

18.7.10 Ensure 'Point and Print Restrictions: When installing drivers for a new connection' is set to 'Enabled: Show warning and elevation prompt' (Automated)

Profile Applicability:

- Level 1 - Member Server
- Level 1 - Domain Controller

Description:

This policy setting controls whether computers will show a warning and a security elevation prompt when users create a new printer connection using Point and Print.

The recommended state for this setting is: **Enabled: Show warning and elevation prompt**.

Note: On August 10, 2021, Microsoft announced a [Point and Print Default Behavior Change](#) which modifies the default Point and Print driver installation and update behavior to require Administrator privileges. This is documented in [KB5005652—Manage new Point and Print default driver installation behavior \(CVE-2021-34481\)](#). This change overrides all Point and Print Group Policy settings and ensures that only Administrators can install printer drivers from a print server using Point and Print.

Rationale:

Enabling Windows User Account Control (UAC) for the installation of new print drivers can help mitigate the PrintNightmare vulnerability ([CVE-2021-34527](#)) and other Print Spooler attacks.

Although the Point and Print default driver installation behavior overrides this setting, it is important to configure this as a backstop in the event that behavior is reversed.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\Software\Policies\Microsoft\Windows  
NT\Printers\PointAndPrint:NoWarningNoElevationOnInstall
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled: Show warning and elevation prompt**:

```
Computer Configuration\Policies\Administrative Templates\Printers\Point and  
Print Restrictions: When installing drivers for a new connection
```

Note: This Group Policy path is provided by the Group Policy template **Printing.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Enabled. (Windows computers will show a warning and a security elevation prompt when users create a new printer connection using Point and Print.)

References:

1. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-1675>
2. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34481>
3. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527>
4. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36958>
5. <https://msrc-blog.microsoft.com/2021/08/10/point-and-print-default-behavior-change/>
6. <https://support.microsoft.com/en-us/topic/kb5005652-manage-new-point-and-print-default-driver-installation-behavior-cve-2021-34481-873642bf-2634-49c5-a23b-6d8e9a302872>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

18.7.11 Ensure 'Point and Print Restrictions: When updating drivers for an existing connection' is set to 'Enabled: Show warning and elevation prompt' (Automated)

Profile Applicability:

- Level 1 - Member Server
- Level 1 - Domain Controller

Description:

This policy setting controls whether computers will show a warning and a security elevation prompt when users are updating drivers for an existing connection using Point and Print.

The recommended state for this setting is: **Enabled: Show warning and elevation prompt**.

Note: On August 10, 2021, Microsoft announced a [Point and Print Default Behavior Change](#) which modifies the default Point and Print driver installation and update behavior to require Administrator privileges. This is documented in [KB5005652—Manage new Point and Print default driver installation behavior \(CVE-2021-34481\)](#). This change overrides all Point and Print Group Policy settings and ensures that only Administrators can install printer drivers from a print server using Point and Print.

Rationale:

Enabling Windows User Account Control (UAC) for updating existing print drivers can help mitigate the PrintNightmare vulnerability ([CVE-2021-34527](#)) and other Print Spooler attacks.

Although the Point and Print default driver installation behavior overrides this setting, it is important to configure this as a backstop in the event that behavior is reversed.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\Software\Policies\Microsoft\Windows  
NT\Printers\PointAndPrint:UpdatePromptSettings
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled: Show warning and elevation prompt**:

```
Computer Configuration\Policies\Administrative Templates\Printers\Point and  
Print Restrictions: When updating drivers for an existing connection
```

Note: This Group Policy path is provided by the Group Policy template **Printing.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Enabled. (Windows computers will show a warning and a security elevation prompt when users are updating drivers for an existing connection using Point and Print.)

References:

1. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-1675>
2. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34481>
3. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527>
4. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36958>
5. <https://msrc-blog.microsoft.com/2021/08/10/point-and-print-default-behavior-change/>
6. <https://support.microsoft.com/en-us/topic/kb5005652-manage-new-point-and-print-default-driver-installation-behavior-cve-2021-34481-873642bf-2634-49c5-a23b-6d8e9a302872>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

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).

18.8.1.1 Ensure 'Turn off notifications network usage' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting blocks applications from using the network to send notifications to update tiles, tile badges, toast, or raw notifications. This policy setting turns off the connection between Windows and the Windows Push Notification Service (WNS). This policy setting also stops applications from being able to poll application services to update tiles.

The recommended state for this setting is: **Enabled**.

Rationale:

Windows Push Notification Services (WNS) is a mechanism to receive third-party notifications and updates from the cloud/Internet. In a high security environment, external systems, especially those hosted outside the organization, should be prevented from having an impact on the secure workstations.

Impact:

Applications and system features will not be able receive notifications from the network from WNS or via notification polling APIs.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\PushNotifications:NoCloudApplicationNotification
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\Start Menu and Taskbar\Turn off notifications network usage
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **WPN.admx/adml** that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

Default Value:

Disabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

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).

18.9.3.1 Ensure 'Include command line in process creation events' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting controls whether the process creation command line text is logged in security audit events when a new process has been created.

The recommended state for this setting is: **Enabled**.

Note: This feature that this setting controls was not originally supported in server OSes older than Windows Server 2012 R2. However, in February 2015 Microsoft added support for the feature to Windows Server 2008 R2 and Windows Server 2012 (non-R2) via an update - [KB3004375](#). Therefore, this setting is also important to set on those older OSes.

Rationale:

Capturing process command line information in event logs can be very valuable when performing forensic investigations of attack incidents.

Impact:

Process command line information will be included in the event logs, which can contain sensitive or private information such as passwords or user data.

Warning: There are potential risks of capturing credentials and sensitive information which could be exposed to users who have read-access to event logs. Microsoft provides a feature called "Protected Event Logging" to better secure event log data. For assistance with protecting event logging, visit: [About Logging Windows - PowerShell | Microsoft Docs](#).

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Audit:ProcessCreationIncludeCmdLine_Enabled
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\System\Audit Process Creation\Include command line in process creation events
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **AuditSettings.admx/adml** that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Disabled. (The process's command line information will not be included in Audit Process Creation events.)

References:

1. https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_logging_windows?view=powershell-7.2#protected-event-logging

Additional Information:

```
Microsoft Windows Server 2016 Security Technical Implementation Guide:  
Version 2, Release 8, Benchmark Date: May 15, 2024
```

```
Vul ID: V-224922  
Rule ID: SV-224922r569186_rule  
STIG ID: WN16-CC-000100  
Severity: CAT II
```


CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.8 <u>Collect Command-Line Audit Logs</u> Collect command-line audit logs. Example implementations include collecting audit logs from PowerShell®, BASH™, and remote administrative terminals.			
v7	8.8 <u>Enable Command-line Audit Logging</u> Enable command-line audit logging for command shells, such as Microsoft Powershell and Bash.			

18.9.4 Credentials Delegation

This section contains settings related to Credential Delegation.

This Group Policy section is provided by the Group Policy template [CredSsp.admx/adml](#) that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.4.1 Ensure 'Encryption Oracle Remediation' is set to 'Enabled: Force Updated Clients' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Some versions of the CredSSP protocol that is used by some applications (such as Remote Desktop Connection) are vulnerable to an encryption oracle attack against the client. This policy controls compatibility with vulnerable clients and servers and allows you to set the level of protection desired for the encryption oracle vulnerability.

The recommended state for this setting is: **Enabled: Force Updated Clients**.

Rationale:

This setting is important to mitigate the CredSSP encryption oracle vulnerability, for which information was published by Microsoft on 03/13/2018 in [CVE-2018-0886 | CredSSP Remote Code Execution Vulnerability](#). All versions of Windows Server from Server 2008 (non-R2) onwards are affected by this vulnerability, and will be compatible with this recommendation provided that they have been patched up through May 2018 (or later).

Impact:

Client applications which use CredSSP will not be able to fall back to the insecure versions and services using CredSSP will not accept unpatched clients. This setting should not be deployed until all remote hosts support the newest version, which is achieved by ensuring that all Microsoft security updates at least through May 2018 are installed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\CredSSP\Parameters:AllowEncryptionOracle
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled: Force Updated Clients**:

Computer Configuration\Policies\Administrative Templates\System\Credentials Delegation\Encryption Oracle Remediation

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **CredSsp.admx/adml** that is included with the Microsoft Windows 10 Release 1803 Administrative Templates (or newer).

Default Value:

Without the May 2018 security update: Enabled: Vulnerable (Client applications which use CredSSP will expose the remote servers to attacks by supporting fall back to the insecure versions and services using CredSSP will accept unpatched clients.)

With the May 2018 security update: Enabled: Mitigated (Client applications which use CredSSP will not be able to fall back to the insecure version but services using CredSSP will accept unpatched clients.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 <u>Enable Anti-Exploitation Features</u> Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	3.4 <u>Deploy Automated Operating System Patch Management Tools</u> Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	●	●	●

18.9.4.2 Ensure 'Remote host allows delegation of non-exportable credentials' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Remote host allows delegation of non-exportable credentials. When using credential delegation, devices provide an exportable version of credentials to the remote host. This exposes users to the risk of credential theft from attackers on the remote host. The Restricted Admin Mode and Windows Defender Remote Credential Guard features are two options to help protect against this risk.

The recommended state for this setting is: **Enabled**.

Note: More detailed information on Windows Defender Remote Credential Guard and how it compares to Restricted Admin Mode can be found at this link: [Protect Remote Desktop credentials with Windows Defender Remote Credential Guard \(Windows 10\) | Microsoft Docs](#)

Rationale:

Restricted Admin Mode was designed to help protect administrator accounts by ensuring that reusable credentials are not stored in memory on remote devices that could potentially be compromised. *Windows Defender Remote Credential Guard* helps you protect your credentials over a Remote Desktop connection by redirecting Kerberos requests back to the device that is requesting the connection. Both features should be enabled and supported, as they reduce the chance of credential theft.

Impact:

The host will support the *Restricted Admin Mode* and *Windows Defender Remote Credential Guard* features.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\CredentialsDelegation:AllowProtectedCreds
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\System\Credentials  
Delegation\Remote host allows delegation of non-exportable credentials
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **CredSsp.admx/adml** that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

Default Value:

Disabled. (*Restricted Admin Mode* and *Windows Defender Remote Credential Guard* are not supported. Users will always need to pass their credentials to the host.)

References:

1. <https://docs.microsoft.com/en-us/windows/security/identity-protection/remote-credential-guard>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	16.5 <u>Encrypt Transmittal of Username and Authentication Credentials</u> Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.		●	●

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).

18.9.5.1 Ensure 'Turn On Virtualization Based Security' is set to 'Enabled' (Automated)

Profile Applicability:

- Next Generation Windows Security - Domain Controller
- Next Generation Windows Security - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting specifies whether Virtualization Based Security is enabled. Virtualization Based Security uses the Windows Hypervisor to provide support for security services.

The recommended state for this setting is: **Enabled**

Note: Virtualization Based Security requires a 64-bit version of Windows with Secure Boot enabled, which in turn requires that Windows was installed with a UEFI BIOS configuration, not a Legacy BIOS configuration. In addition, if running Windows on a virtual machine, the hardware-assisted CPU virtualization feature (Intel VT-x or AMD-V) must be exposed by the host to the guest VM.

More information on system requirements for this feature can be found at [Windows Defender Credential Guard Requirements \(Windows 10\) | Microsoft Docs](#)

Note #2: Credential Guard and Device Guard are not currently supported when using Azure IaaS VMs.

Rationale:

Kerberos, NTLM, and Credential manager isolate secrets by using virtualization-based security. Previous versions of Windows stored secrets in the Local Security Authority (LSA). Prior to Windows 10, the LSA stored secrets used by the operating system in its process memory. With Windows Defender Credential Guard enabled, the LSA process in the operating system talks to a new component called the isolated LSA process that stores and protects those secrets. Data stored by the isolated LSA process is protected using virtualization-based security and is not accessible to the rest of the operating system.

Impact:

Warning: All drivers on the system must be compatible with this feature or the system may crash. Ensure that this policy setting is only deployed to computers which are known to be compatible.

Warning #2: Enabling Windows Defender Credential Guard on Domain Controllers is not supported. The domain controller hosts authentication services which integrate with processes isolated when Windows Defender Credential Guard is enabled, causing crashes.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard\EnableVirtualizationBasedSecurity
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\System\Device Guard\Turn On Virtualization Based Security
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **DeviceGuard.admx/adml** that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

Default Value:

Disabled.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224923
Rule ID: SV-224923r857253_rule
STIG ID: WN16-CC-000110
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 <u>Enable Anti-Exploitation Features</u> Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.			
v7	8.3 <u>Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies</u> Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.			

18.9.5.2 Ensure 'Turn On Virtualization Based Security: Select Platform Security Level' is set to 'Secure Boot' or higher (Automated)

Profile Applicability:

- Next Generation Windows Security - Domain Controller
- Next Generation Windows Security - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting specifies whether Virtualization Based Security (VBS) is enabled. VBS uses the Windows Hypervisor to provide support for security services.

The recommended state for this setting is: **Secure Boot** or **Secure Boot and DMA Protection**.

Note: VBS requires a 64-bit version of Windows with Secure Boot enabled, which in turn requires that Windows was installed with a UEFI BIOS configuration, not a Legacy BIOS configuration. In addition, if running Windows on a virtual machine, the hardware-assisted CPU virtualization feature (Intel VT-x or AMD-V) must be exposed by the host to the guest VM.

More information on system requirements for this feature can be found at [Windows Defender Credential Guard Requirements \(Windows 10\) | Microsoft Docs](#)

Note #2: Credential Guard and Device Guard are not currently supported when using Azure IaaS VMs.

Rationale:

Secure Boot can help reduce the risk of bootloader attacks and in conjunction with DMA protections to help protect data from being scraped from memory.

Impact:

Choosing the **Secure Boot** option provides the system with as much protection as is supported by the computer's hardware. A system with input/output memory management units (IOMMUs) will have Secure Boot with DMA protection. A system without IOMMUs will simply have Secure Boot enabled without DMA protection.

Choosing the **Secure Boot with DMA protection** option requires the system to have IOMMUs in order to enable VBS. Without IOMMU hardware support, VBS will be disabled.

Warning: All drivers on the system must be compatible with this feature or the system may crash. Ensure that this policy setting is only deployed to computers which are known to be compatible.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1** or **3**.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard:RequirePlatformSecurityFeatures
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Secure Boot** or **Secure Boot and DMA Protection**:

```
Computer Configuration\Policies\Administrative Templates\System\DeviceGuard\Turn On Virtualization Based Security: Select Platform Security Level
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **DeviceGuard.admx/adml** that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

Default Value:

Disabled.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224923 and V-224864

Rule ID: SV-224923r857253_rule and SV-224864r569186_rule

STIG ID: WN16-CC-000110 and WN16-00-000470

Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 <u>Enable Anti-Exploitation Features</u> Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.			
v7	8.3 <u>Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies</u> Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.			

18.9.5.3 Ensure 'Turn On Virtualization Based Security: Virtualization Based Protection of Code Integrity' is set to 'Enabled with UEFI lock' (Automated)

Profile Applicability:

- Next Generation Windows Security - Domain Controller
- Next Generation Windows Security - Member Server

Description:

This setting enables virtualization based protection of Kernel Mode Code Integrity. When this is enabled, kernel mode memory protections are enforced and the Code Integrity validation path is protected by the Virtualization Based Security feature.

The recommended state for this setting is: **Enabled with UEFI lock**

Note: Virtualization Based Security requires a 64-bit version of Windows with Secure Boot enabled, which in turn requires that Windows was installed with a UEFI BIOS configuration, not a Legacy BIOS configuration. In addition, if running Windows on a virtual machine, the hardware-assisted CPU virtualization feature (Intel VT-x or AMD-V) must be exposed by the host to the guest VM.

More information on system requirements for this feature can be found at [Windows Defender Credential Guard Requirements \(Windows 10\) | Microsoft Docs](#)

Note #2: Credential Guard and Device Guard are not currently supported when using Azure IaaS VMs.

Rationale:

The **Enabled with UEFI lock** option ensures that Virtualization Based Protection of Code Integrity cannot be disabled remotely.

Impact:

Warning: All drivers on the system must be compatible with this feature or the system may crash. Ensure that this policy setting is only deployed to computers which are known to be compatible.

Warning #2: Once this setting is turned on and active, **Virtualization Based Security cannot be disabled solely via GPO** or any other remote method. After removing the setting from GPO, the features must also be manually disabled *locally at the machine* using the steps provided at this link:

[Manage Windows Defender Credential Guard \(Windows 10\) | Microsoft Docs](#)

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard:HypervisorEnforcedCodeIntegrity
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled with UEFI lock**:

```
Computer Configuration\Policies\Administrative Templates\System\DeviceGuard\Turn On Virtualization Based Security: Virtualization Based Protection of Code Integrity
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **DeviceGuard.admx/adml** that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

Default Value:

Disabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 <u>Enable Anti-Exploitation Features</u> Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 <u>Enable Operating System Anti-Exploitation Features/Deploy Anti-Exploit Technologies</u> Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

18.9.5.4 Ensure 'Turn On Virtualization Based Security: Require UEFI Memory Attributes Table' is set to 'True (checked)' (Automated)

Profile Applicability:

- Next Generation Windows Security - Domain Controller
- Next Generation Windows Security - Member Server

Description:

This option will only enable Virtualization Based Protection of Code Integrity on devices with UEFI firmware support for the Memory Attributes Table. Devices without the UEFI Memory Attributes Table may have firmware that is incompatible with Virtualization Based Protection of Code Integrity which in some cases can lead to crashes or data loss or incompatibility with certain plug-in cards. If not setting this option the targeted devices should be tested to ensure compatibility.

The recommended state for this setting is: **True (checked)**

Note: Virtualization Based Security requires a 64-bit version of Windows with Secure Boot enabled, which in turn requires that Windows was installed with a UEFI BIOS configuration, not a Legacy BIOS configuration. In addition, if running Windows on a virtual machine, the hardware-assisted CPU virtualization feature (Intel VT-x or AMD-V) must be exposed by the host to the guest VM.

More information on system requirements for this feature can be found at [Windows Defender Credential Guard Requirements \(Windows 10\) | Microsoft Docs](#)

Note #2: Credential Guard and Device Guard are not currently supported when using Azure IaaS VMs.

Rationale:

This setting will help protect this control from being enabled on a system that is not compatible which could lead to a crash or data loss.

Impact:

Warning: All drivers on the system must be compatible with this feature or the system may crash. Ensure that this policy setting is only deployed to computers which are known to be compatible.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard:HVCIMATRequired
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **TRUE**:

```
Computer Configuration\Policies\Administrative Templates\System\Device  
Guard\Turn On Virtualization Based Security: Require UEFI Memory Attributes  
Table
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **DeviceGuard.admx/adml** that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

Default Value:

Disabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 <u>Enable Anti-Exploitation Features</u> Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 <u>Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies</u> Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

18.9.5.5 Ensure 'Turn On Virtualization Based Security: Credential Guard Configuration' is set to 'Enabled with UEFI lock' (MS Only) (Automated)

Profile Applicability:

- Next Generation Windows Security - Member Server
- STIG Member Server

Description:

This setting lets users turn on Credential Guard with virtualization-based security to help protect credentials. The "Enabled with UEFI lock" option ensures that Credential Guard cannot be disabled remotely. In order to disable the feature, you must set the Group Policy to "Disabled" as well as remove the security functionality from each computer, with a physically present user, in order to clear configuration persisted in UEFI.

The recommended state for this setting is: **Enabled with UEFI lock**, but only on Member Servers (not Domain Controllers).

Note: Virtualization Based Security requires a 64-bit version of Windows with Secure Boot enabled, which in turn requires that Windows was installed with a UEFI BIOS configuration, not a Legacy BIOS configuration. In addition, if running Windows on a virtual machine, the hardware-assisted CPU virtualization feature (Intel VT-x or AMD-V) must be exposed by the host to the guest VM.

More information on system requirements for this feature can be found at [Windows Defender Credential Guard Requirements \(Windows 10\) | Microsoft Docs](#)

Note #2: Credential Guard and Device Guard are not currently supported when using Azure IaaS VMs.

Rationale:

The **Enabled with UEFI lock** option ensures that Credential Guard cannot be disabled remotely.

Impact:

Warning: All drivers on the system must be compatible with this feature or the system may crash. Ensure that this policy setting is only deployed to computers which are known to be compatible.

Warning #2: Enabling Windows Defender Credential Guard on Domain Controllers is not supported. The domain controller hosts authentication services which integrate with processes isolated when Windows Defender Credential Guard is enabled, causing crashes.

Warning #3: Once this setting is turned on and active, **Credential Guard cannot be disabled solely via GPO** or any other remote method. After removing the setting from GPO, the features must also be manually disabled *locally at the machine* using the steps provided at this link:

[Manage Windows Defender Credential Guard \(Windows 10\) | Microsoft Docs](#)

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard:LsaCfgFlags
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled with UEFI lock** (on Member Servers only):

```
Computer Configuration\Policies\Administrative Templates\System\Device Guard\Turn On Virtualization Based Security: Credential Guard Configuration
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **DeviceGuard.admx/adml** that is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).

Default Value:

Disabled.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225012
Rule ID: SV-225012r902427_rule
STIG ID: WN16-MS-000120
Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 <u>Enable Anti-Exploitation Features</u> Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.			
v7	8.3 <u>Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies</u> Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.			

18.9.5.6 Ensure 'Turn On Virtualization Based Security: Credential Guard Configuration' is set to 'Disabled' (DC Only) (Automated)

Profile Applicability:

- Next Generation Windows Security - Domain Controller

Description:

This setting lets users turn on Credential Guard with virtualization-based security to help protect credentials.

The recommended state for this setting is: **Disabled** on Domain Controllers.

Note: Virtualization Based Security requires a 64-bit version of Windows with Secure Boot enabled, which in turn requires that Windows was installed with a UEFI BIOS configuration, not a Legacy BIOS configuration. In addition, if running Windows on a virtual machine, the hardware-assisted CPU virtualization feature (Intel VT-x or AMD-V) must be exposed by the host to the guest VM.

More information on system requirements for this feature can be found at [Windows Defender Credential Guard Requirements \(Windows 10\) | Microsoft Docs](#)

Note #2: Credential Guard and Device Guard are not currently supported when using Azure IaaS VMs.

Rationale:

Credential Guard is not useful on Domain Controllers and can cause crashes on them.

Impact:

None - this is the default behavior.

Warning: Enabling Windows Defender Credential Guard on Domain Controllers is not supported. The domain controller hosts authentication services which integrate with processes isolated when Windows Defender Credential Guard is enabled, causing crashes.

[Manage Windows Defender Credential Guard \(Windows 10\) | Microsoft Docs](#)

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

HKLM\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard:LsaCfgFlags

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

Computer Configuration\Policies\Administrative Templates\System\Device Guard\Turn On Virtualization Based Security: Credential Guard Configuration

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **DeviceGuard.admx/adml** that is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).

Default Value:

Disabled. (Credential Guard is disabled.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 <u>Enable Anti-Exploitation Features</u> Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.			
v7	8.3 <u>Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies</u> Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.			

18.9.5.7 Ensure 'Turn On Virtualization Based Security: Secure Launch Configuration' is set to 'Enabled' (Automated)

Profile Applicability:

- Next Generation Windows Security - Domain Controller
- Next Generation Windows Security - Member Server

Description:

Secure Launch protects the Virtualization Based Security environment from exploited vulnerabilities in device firmware.

The recommended state for this setting is: **Enabled**.

Note: Virtualization Based Security requires a 64-bit version of Windows with Secure Boot enabled, which in turn requires that Windows was installed with a UEFI BIOS configuration, not a Legacy BIOS configuration. In addition, if running Windows on a virtual machine, the hardware-assisted CPU virtualization feature (Intel VT-x or AMD-V) must be exposed by the host to the guest VM.

More information on system requirements for this feature can be found at [Windows Defender Credential Guard Requirements \(Windows 10\) | Microsoft Docs](#)

Note #2: Credential Guard and Device Guard are not currently supported when using Azure IaaS VMs.

Rationale:

Secure Launch changes the way windows boots to use Intel Trusted Execution Technology (TXT) and Runtime BIOS Resilience features to prevent firmware exploits from being able to impact the security of the Windows Virtualization Based Security environment.

Impact:

Warning: All drivers on the system must be compatible with this feature or the system may crash. Ensure that this policy setting is only deployed to computers which are known to be compatible.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

HKLM\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard:ConfigureSystemGuardLaunch

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

Computer Configuration\Policies\Administrative Templates\System\Device Guard\Turn On Virtualization Based Security: Secure Launch Configuration

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **DeviceGuard.admx/adml** that is included with the Microsoft Windows 10 Release 1809 & Server 2019 Administrative Templates (or newer).

Default Value:

Not Configured. (Administrative users can choose whether to enable or disable Secure Launch.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 <u>Enable Anti-Exploitation Features</u> Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 <u>Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies</u> Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

18.9.6 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 is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template [DeviceInstallation.admx/adml](#) that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.7.2 Ensure 'Prevent device metadata retrieval from the Internet' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to prevent Windows from retrieving device metadata from the Internet.

The recommended state for this setting is: **Enabled**.

Note: This will not prevent the installation of basic hardware drivers, but does prevent associated third-party utility software from automatically being installed under the context of the **SYSTEM** account.

Rationale:

Installation of software should be conducted by an authorized system administrator and not a standard user. Allowing automatic third-party software installations under the context of the **SYSTEM** account has potential for allowing unauthorized access via backdoors or installation software bugs.

Impact:

Standard users without administrator privileges will not be able to install associated third-party utility software for peripheral devices. This may limit the use of advanced features of those devices unless/until an administrator installs the associated utility software for the device.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Device  
Metadata:PreventDeviceMetadataFromNetwork
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

Computer Configuration\Policies\Administrative Templates\System\Device Installation\Prevent device metadata retrieval from the Internet

Note: This Group Policy path is provided by the Group Policy template **DeviceInstallation.admx/adml** that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates, or with the Group Policy template **DeviceSetup.admx/adml** that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (The setting in the Device Installation Settings dialog box controls whether Windows retrieves device metadata from the Internet.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.5 Allowlist Authorized Software Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.		●	●
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	18.3 Verify That Acquired Software is Still Supported Verify that the version of all software acquired from outside your organization is still supported by the developer or appropriately hardened based on developer security recommendations.		●	●

18.9.8 Disk NV Cache

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template **DiskNVCache.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.9 Disk Quotas

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template **DiskQuota.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.10 Display

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template **Display.admx/adml** that is included with the Microsoft Windows 10 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).

18.9.13.1 Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good, unknown and bad but critical' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to specify which boot-start drivers are initialized based on a classification determined by an Early Launch Antimalware boot-start driver. The Early Launch Antimalware boot-start driver can return the following classifications for each boot-start driver:

- **Good:** The driver has been signed and has not been tampered with.
- **Bad:** The driver has been identified as malware. It is recommended that you do not allow known bad drivers to be initialized.
- **Bad, but required for boot:** The driver has been identified as malware, but the computer cannot successfully boot without loading this driver.
- **Unknown:** This driver has not been attested to by your malware detection application and has not been classified by the Early Launch Antimalware boot-start driver.

If you enable this policy setting you will be able to choose which boot-start drivers to initialize the next time the computer is started.

If your malware detection application does not include an Early Launch Antimalware boot-start driver or if your Early Launch Antimalware boot-start driver has been disabled, this setting has no effect and all boot-start drivers are initialized.

The recommended state for this setting is: **Enabled: Good, unknown and bad but critical.**

Rationale:

This policy setting helps reduce the impact of malware that has already infected your system.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **3**.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Policies\EarlyLaunch:DriverLoadPolicy
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled: Good, unknown and bad but critical**:

```
Computer Configuration\Policies\Administrative Templates\System\Early Launch Antimalware\Boot-Start Driver Initialization Policy
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **EarlyLaunchAM.admx/adml** that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (Boot-start drivers determined to be Good, Unknown or Bad but Boot Critical are initialized and the initialization of drivers determined to be bad is skipped.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 <u>Enable Anti-Exploitation Features</u> Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 <u>Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies</u> Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

18.9.13.2 Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: any, but ALL' (STIG only) (Automated)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting allows you to specify which boot-start drivers are initialized based on a classification determined by an Early Launch Antimalware boot-start driver. The Early Launch Antimalware boot-start driver can return the following classifications for each boot-start driver:

- **Good:** The driver has been signed and has not been tampered with.
- **Bad:** The driver has been identified as malware. It is recommended that you do not allow known bad drivers to be initialized.
- **Bad, but required for boot:** The driver has been identified as malware, but the computer cannot successfully boot without loading this driver.
- **Unknown:** This driver has not been attested to by your malware detection application and has not been classified by the Early Launch Antimalware boot-start driver.

If you enable this policy setting you will be able to choose which boot-start drivers to initialize the next time the computer is started.

If your malware detection application does not include an Early Launch Antimalware boot-start driver or if your Early Launch Antimalware boot-start driver has been disabled, this setting has no effect and all boot-start drivers are initialized.

The recommended state for this setting is: **Enabled: any, but ALL.**

Rationale:

This policy setting helps reduce the impact of malware that has already infected your system.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1, 3, or 8**.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Policies\EarlyLaunch:DriverLoadPolicy
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled: Any, but ALL**:

```
Computer Configuration\Policies\Administrative Templates\System\Early Launch Antimalware\Boot-Start Driver Initialization Policy
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **EarlyLaunchAM.admx/adml** that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (Boot-start drivers determined to be Good, Unknown or Bad but Boot Critical are initialized and the initialization of drivers determined to be bad is skipped.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224924
Rule ID: SV-224924r569186_rule
STIG ID: WN16-CC-000140
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 <u>Enable Anti-Exploitation Features</u> Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 <u>Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies</u> Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

18.9.14 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 Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

The "Do not apply during periodic background processing" option prevents the system from updating affected registry policies in the background while the computer is in use. When background updates are disabled, registry policy changes will not take effect until the next user logon or system restart.

This setting affects all policy settings within the Administrative Templates folder and any other policies that store values in the registry.

The recommended state for this setting is: **Enabled: FALSE** (unchecked).

Rationale:

Setting this option to false (unchecked) will ensure that domain registry policy changes are applied more quickly, as compared to waiting until the next user logon or system restart.

Impact:

Group Policy settings within the Administrative Templates folder (and other policies that store values in the registry) will be reapplied even when the system is in use, which may have a slight impact on performance.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Group Policy\{35378EAC-683F-11D2-A89A-00C04FBBCEFA2}:NoBackgroundPolicy
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**, then set the **Do not apply during periodic background processing** option to **FALSE** (unchecked):

Computer Configuration\Policies\Administrative Templates\System\Group Policy\Configure registry policy processing

Note: This Group Policy path is provided by the Group Policy template **GroupPolicy.admx/adml** that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (Group policies are not reapplied until the next logon or restart.)

References:

1. [https://learn.microsoft.com/en-us/previous-versions/ms813374\(v=msdn.10\)?redirectedfrom=MSDN](https://learn.microsoft.com/en-us/previous-versions/ms813374(v=msdn.10)?redirectedfrom=MSDN)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	5.4 Deploy System Configuration Management Tools Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.			

18.9.19.3 Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

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.

Impact:

Group Policy settings within the Administrative Templates folder (and other policies that store values in the registry) will be reapplied even if they have not been changed, which may cause Group Policy refreshes to take longer.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Group Policy\{35378EAC-683F-11D2-A89A-00C04FBBCFA2}:NoGPListChanges
```

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).

Default Value:

Disabled. (Group policies are not reapplied if they have not been changed.)

References:

1. [https://learn.microsoft.com/en-us/previous-versions/ms813374\(v=msdn.10\)?redirectedfrom=MSDN](https://learn.microsoft.com/en-us/previous-versions/ms813374(v=msdn.10)?redirectedfrom=MSDN)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224925
Rule ID: SV-224925r569186_rule
STIG ID: WN16-CC-000150
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.4 <u>Deploy System Configuration Management Tools</u> Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.		●	●

18.9.19.4 Ensure 'Configure security policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

The "Do not apply during periodic background processing" option prevents the system from updating affected security policies in the background while the computer is in use. When background updates are disabled, updates to security policies will not take effect until the next user logon or system restart.

This setting affects all policy settings that use the built-in security template of Group Policy (e.g. Windows Settings\Security Settings).

The recommended state for this setting is: **Enabled: FALSE** (unchecked).

Rationale:

Setting this option to false (unchecked) will ensure that domain security policy changes are applied more quickly, as compared to waiting until the next user logon or system restart.

Impact:

Built-in security template settings will be reapplied by Group Policy even when the system is in use, which may have a slight impact on performance.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Group Policy\{827D319E-6EAC-11D2-A4EA-00C04F79F83A}:NoBackgroundPolicy
```


Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**, then set the **Do not apply during periodic background processing** option to **FALSE** (unchecked):

Computer Configuration\Policies\Administrative Templates\System\Group Policy\Configure security policy processing

Note: This Group Policy path is provided by the Group Policy template **GroupPolicy.admx/adml** that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (Group policies are not reapplied until the next logon or restart.)

References:

1. [https://learn.microsoft.com/en-us/previous-versions/ms813374\(v=msdn.10\)?redirectedfrom=MSDN](https://learn.microsoft.com/en-us/previous-versions/ms813374(v=msdn.10)?redirectedfrom=MSDN)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	5.4 Deploy System Configuration Management Tools Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.			

18.9.19.5 Ensure 'Configure security policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

The "Process even if the Group Policy objects have not changed" option updates and reapplies security policies even if the security policies have not changed.

This setting affects all policy settings within the built-in security template of Group Policy (e.g. Windows Settings\Security Settings).

The recommended state for this setting is: **Enabled: TRUE** (checked).

Rationale:

Setting this option to true (checked) will ensure unauthorized local changes are reverted to match the domain-based Group Policy settings.

Impact:

Built-in security template settings will be reapplied even if they have not been changed, which may cause Group Policy refreshes to take longer.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Group Policy\{827D319E-6EAC-11D2-A4EA-00C04F79F83A}:NoGPListChanges
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**, then set the **Process even if the Group Policy objects have not changed** option to **TRUE** (checked):

```
Computer Configuration\Policies\Administrative Templates\System\Group Policy\Configure security policy processing
```

Note: This Group Policy path is provided by the Group Policy template **GroupPolicy.admx/adml** that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (Group policies are not reapplied if they have not been changed.)

References:

1. [https://learn.microsoft.com/en-us/previous-versions/ms813374\(v=msdn.10\)?redirectedfrom=MSDN](https://learn.microsoft.com/en-us/previous-versions/ms813374(v=msdn.10)?redirectedfrom=MSDN)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	5.4 <u>Deploy System Configuration Management Tools</u> Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.			

18.9.19.6 Ensure 'Continue experiences on this device' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether the Windows device is allowed to participate in cross-device experiences (continue experiences).

The recommended state for this setting is: **Disabled**.

Rationale:

A cross-device experience is when a system can access app and send messages to other devices. In an enterprise managed environment only trusted systems should be communicating within the network. Access to any other system should be prohibited.

Impact:

The Windows device will not be discoverable by other devices, and cannot participate in cross-device experiences.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\System:EnableCdp
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Administrative Templates\System\Group Policy\Continue experiences on this device
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **GroupPolicy.admx/adml** that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

Default Value:

The default behavior depends on the Windows edition.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

18.9.19.7 Ensure 'Turn off background refresh of Group Policy' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting prevents Group Policy from being updated while the computer is in use. This policy setting applies to Group Policy for computers, users and Domain Controllers.

The recommended state for this setting is: **Disabled**.

Rationale:

This setting ensures that group policy changes take effect more quickly, as compared to waiting until the next user logon or system restart.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location and when set properly a value **does not exist**.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:
DisableBkGndGroupPolicy
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Administrative Templates\System\Group
Policy\Turn off background refresh of Group Policy
```

Note: This Group Policy path is provided by the Group Policy template **GroupPolicy.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Updates can be applied while users are working.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	5.4 <u>Deploy System Configuration Management Tools</u> Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.			

18.9.20 Internet Communication Management

This section contains recommendations related to Internet Communication Management.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.20.1 Internet Communication settings

This section contains recommendations related to Internet Communication settings.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.20.1.1 Ensure 'Turn off downloading of print drivers over HTTP' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting controls whether the computer can download print driver packages over HTTP. To set up HTTP printing, printer drivers that are not available in the standard operating system installation might need to be downloaded over HTTP.

The recommended state for this setting is: **Enabled**.

Rationale:

Users might download drivers that include malicious code.

Impact:

Print drivers cannot be downloaded over HTTP.

Note: This policy setting does not prevent the client computer from printing to printers on the intranet or the Internet over HTTP. It only prohibits downloading drivers that are not already installed locally.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Printers:DisableWebPnPDownload
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\System\Internet  
Communication Management\Internet Communication settings\Turn off downloading  
of print drivers over HTTP
```

Note: This Group Policy path is provided by the Group Policy template **ICM.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Users can download print drivers over HTTP.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224926
Rule ID: SV-224926r569186_rule
STIG ID: WN16-CC-000160
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.5 Allowlist Authorized Software Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.			
v7	2.7 Utilize Application Whitelisting Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.			

18.9.20.1.2 Ensure 'Turn off handwriting personalization data sharing' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This setting turns off data sharing from the handwriting recognition personalization tool.

The handwriting recognition personalization tool enables Tablet PC users to adapt handwriting recognition to their own writing style by providing writing samples. The tool can optionally share user writing samples with Microsoft to improve handwriting recognition in future versions of Windows. The tool generates reports and transmits them to Microsoft over a secure connection.

The recommended state for this setting is: **Enabled**.

Rationale:

A person's handwriting is Personally Identifiable Information (PII), especially when it comes to your signature. As such, it is unacceptable in many environments to automatically upload PII to a website without explicit approval by the user.

Impact:

Tablet PC users cannot choose to share writing samples from the handwriting recognition personalization tool with Microsoft.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

HKLM\SOFTWARE\Policies\Microsoft\Windows\TabletPC:PreventHandwritingDataSharing

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off handwriting personalization data sharing

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **ShapeCollector.admx/adml** that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

Tablet PC users can choose whether or not they want to share their writing samples from the handwriting recognition personalization tool with Microsoft.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

18.9.20.1.3 Ensure 'Turn off handwriting recognition error reporting' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

Turns off the handwriting recognition error reporting tool.

The handwriting recognition error reporting tool enables users to report errors encountered in Tablet PC Input Panel. The tool generates error reports and transmits them to Microsoft over a secure connection. Microsoft uses these error reports to improve handwriting recognition in future versions of Windows.

The recommended state for this setting is: **Enabled**.

Rationale:

A person's handwriting is Personally Identifiable Information (PII), especially when it comes to your signature. As such, it is unacceptable in many environments to automatically upload PII to a website without explicit approval by the user.

Impact:

Users cannot start the handwriting recognition error reporting tool or send error reports to Microsoft.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\HandwritingErrorReports:PreventHandwritingErrorReports
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off handwriting recognition error reporting
```

Note: This Group Policy path is provided by the Group Policy template **InkWatson.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Tablet PC users can report handwriting recognition errors to Microsoft.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

18.9.20.1.4 Ensure 'Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting specifies whether the Internet Connection Wizard can connect to Microsoft to download a list of Internet Service Providers (ISPs).

The recommended state for this setting is: **Enabled**.

Rationale:

In an enterprise managed environment we want to lower the risk of a user unknowingly exposing sensitive data.

Impact:

The "Choose a list of Internet Service Providers" path in the Internet Connection Wizard causes the wizard to exit. This prevents users from retrieving the list of ISPs, which resides on Microsoft servers.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Internet Connection  
Wizard:ExitOnMSICW
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\System\Internet  
Communication Management\Internet Communication settings\Turn off Internet  
Connection Wizard if URL connection is referring to Microsoft.com
```

Note: This Group Policy path is provided by the Group Policy template **ICM.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Users can connect to Microsoft to download a list of ISPs for their area.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

18.9.20.1.5 Ensure 'Turn off Internet download for Web publishing and online ordering wizards' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls whether Windows will download a list of providers for the Web publishing and online ordering wizards.

The recommended state for this setting is: **Enabled**.

Rationale:

Although the risk is minimal, enabling this setting will reduce the possibility of a user unknowingly downloading malicious content through this feature.

Impact:

Windows is prevented from downloading providers; only the service providers cached in the local registry are displayed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoWebServices
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Internet download for Web publishing and online ordering wizards
```

Note: This Group Policy path is provided by the Group Policy template **ICM.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (A list of providers is downloaded when the user uses the web publishing or online ordering wizards.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

18.9.20.1.6 Ensure 'Turn off printing over HTTP' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting allows you to disable the client computer's ability to print over HTTP, which allows the computer to print to printers on the intranet as well as the Internet.

The recommended state for this setting is: **Enabled**.

Note: This control affects printing over **both** HTTP and HTTPS.

Rationale:

Information that is transmitted over HTTP through this capability is not protected and can be intercepted by malicious users. For this reason, it is not often used in enterprise managed environments.

Impact:

The client computer will not be able to print to Internet printers over HTTP or HTTPS.

Note: This policy setting affects the client side of Internet printing only. Regardless of how it is configured, a computer could act as an Internet Printing server and make its shared printers available through HTTP.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Printers:DisableHTTPPrinting

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off printing over HTTP

Note: This Group Policy path is provided by the Group Policy template **ICM.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Users can choose to print to Internet printers over HTTP.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224927
Rule ID: SV-224927r569186_rule
STIG ID: WN16-CC-000170
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<u>13.3 Monitor and Block Unauthorized Network Traffic</u> Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.			●

18.9.20.1.7 Ensure 'Turn off Registration if URL connection is referring to Microsoft.com' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting specifies whether the Windows Registration Wizard connects to Microsoft.com for online registration.

The recommended state for this setting is: **Enabled**.

Rationale:

Users in an enterprise managed environment should not be registering their own copies of Windows, providing their own PII in the process.

Impact:

Users are blocked from connecting to Microsoft.com for online registration and they cannot register their copy of Windows online.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Registration Wizard  
Control:NoRegistration
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\System\Internet  
Communication Management\Internet Communication settings\Turn off  
Registration if URL connection is referring to Microsoft.com
```

Note: This Group Policy path is provided by the Group Policy template **ICM.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Users can connect to Microsoft.com to complete the online Windows Registration.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

18.9.20.1.8 Ensure 'Turn off Search Companion content file updates' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting specifies whether Search Companion should automatically download content updates during local and Internet searches.

The recommended state for this setting is: **Enabled**.

Rationale:

There is a small risk that users will unknowingly reveal sensitive information because of the topics they are searching for. This risk is very low because even if this setting is enabled users still must submit search queries to the desired search engine in order to perform searches.

Impact:

Search Companion does not download content updates during searches.

Note: Internet searches will still send the search text and information about the search to Microsoft and the chosen search provider. If you select Classic Search, the Search Companion feature will be unavailable. You can select Classic Search by clicking Start, Search, Change Preferences, and then Change Internet Search Behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

HKLM\SOFTWARE\Policies\Microsoft\SearchCompanion:DisableContentFileUpdates

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Search Companion content file updates

Note: This Group Policy path is provided by the Group Policy template **ICM.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Search Companion downloads content updates unless the user is using Classic Search.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

18.9.20.1.9 Ensure 'Turn off the "Order Prints" picture task' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting specifies whether the "Order Prints Online" task is available from Picture Tasks in Windows folders.

The Order Prints Online Wizard is used to download a list of providers and allow users to order prints online.

The recommended state for this setting is: **Enabled**.

Rationale:

In an enterprise managed environment we want to lower the risk of a user unknowingly exposing sensitive data.

Impact:

The task "Order Prints Online" is removed from Picture Tasks in File Explorer folders.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer:NoOnlinePrintsWizard
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off the "Order Prints" picture task
```

Note: This Group Policy path is provided by the Group Policy template **ICM.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (The "Order Prints Online" task is displayed in Picture Tasks in File Explorer folders.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

18.9.20.1.10 Ensure 'Turn off the "Publish to Web" task for files and folders' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting specifies whether the tasks Publish this file to the Web, Publish this folder to the Web, and Publish the selected items to the Web are available from File and Folder Tasks in Windows folders.

The recommended state for this setting is: **Enabled**.

Rationale:

Users may publish confidential or sensitive information to a public service outside of the control of the organization.

Impact:

The "Publish to Web" task is removed from File and Folder tasks in Windows folders.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer:NoPublishing Wizard
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off the "Publish to Web" task for files and folders
```

Note: This Group Policy path is provided by the Group Policy template **ICM.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (The "Publish to Web" task is shown in File and Folder tasks in Windows folders.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

18.9.20.1.11 Ensure 'Turn off the Windows Messenger Customer Experience Improvement Program' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting specifies whether Windows Messenger can collect anonymous information about how the Windows Messenger software and service is used. Microsoft uses information collected through the Customer Experience Improvement Program to detect software flaws so that they can be corrected more quickly, enabling this setting will reduce the amount of data Microsoft is able to gather for this purpose.

The recommended state for this setting is: **Enabled**.

Rationale:

Large enterprise managed environments may not want to have information collected by Microsoft from managed client computers.

Impact:

Windows Messenger will not collect usage information, and the user settings to enable the collection of usage information will not be shown.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **2**.

```
HKLM\SOFTWARE\Policies\Microsoft\Messenger\Client:CEIP
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off the Windows Messenger Customer Experience Improvement Program
```

Note: This Group Policy path is provided by the Group Policy template **ICM.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Users have the choice to opt-in and allow information to be collected.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

18.9.20.1.12 Ensure 'Turn off Windows Customer Experience Improvement Program' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting specifies whether the Windows Customer Experience Improvement Program can collect anonymous information about how Windows is used.

Microsoft uses information collected through the Windows Customer Experience Improvement Program to improve features that are most used and to detect flaws so that they can be corrected more quickly. Enabling this setting will reduce the amount of data Microsoft is able to gather for this purpose. The recommended state for this setting is: **Enabled**.

Rationale:

Large enterprise managed environments may not want to have information collected by Microsoft from managed client computers.

Impact:

All users are opted out of the Windows Customer Experience Improvement Program.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\SQMClient\Windows:CEIPEnable
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\System\Internet  
Communication Management\Internet Communication settings\Turn off Windows  
Customer Experience Improvement Program
```

Note: This Group Policy path is provided by the Group Policy template **ICM.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

The Administrator can use the Problem Reports and Solutions component in Control Panel to enable Windows Customer Experience Improvement Program for all users.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

18.9.20.1.13 Ensure 'Turn off Windows Error Reporting' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting controls whether or not errors are reported to Microsoft.

Error Reporting is used to report information about a system or application that has failed or has stopped responding and is used to improve the quality of the product.

The recommended state for this setting is: **Enabled**.

Rationale:

If a Windows Error occurs in a secure, enterprise managed environment, the error should be reported directly to IT staff for troubleshooting and remediation. There is no benefit to the corporation to report these errors directly to Microsoft, and there is some risk of unknowingly exposing sensitive data as part of the error.

Impact:

Users are not given the option to report errors to Microsoft.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0** (DoReport) and **1** (Disabled).

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows Error  
Reporting:Disabled  
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\PCHealth\ErrorReporting:DoRepo  
rt
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\System\Internet  
Communication Management\Internet Communication settings\Turn off Windows  
Error Reporting
```

Note: This Group Policy path is provided by the Group Policy template **ICM.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Errors may be reported to Microsoft via the Internet or to a corporate file share.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

18.9.21 iSCSI

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template [iSCSI.admx/adml](#) that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.22 KDC

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template [KDC.admx/adml](#) that is included with the Microsoft Windows Server 2008 (non-R2) Administrative Templates (or newer).

18.9.23 Kerberos

This section contains recommendations for Kerberos settings.

This Group Policy section is provided by the Group Policy template [Kerberos.admx/adml](#) that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.23.1 Ensure 'Support device authentication using certificate' is set to 'Enabled: Automatic' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting allows you to set support for Kerberos to attempt authentication using the certificate for the device to the domain.

Support for device authentication using certificate will require connectivity to a DC in the device account domain which supports certificate authentication for computer accounts.

The recommended state for this setting is: **Enabled: Automatic**.

Rationale:

Having stronger device authentication with the use of certificates is strongly encouraged over standard username and password authentication. Having this set to Automatic will allow certificate based authentication to be used whenever possible.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0** (DevicePKInitBehavior) and **1** (DevicePKInitEnabled).

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\kerberos\parameters:DevicePKInitBehavior  
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\kerberos\parameters:DevicePKInitEnabled
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled: Automatic**:

```
Computer Configuration\Policies\Administrative  
Templates\System\Kerberos\Support device authentication using certificate
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **Kerberos.admx/adml** that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

Default Value:

Automatic. (Devices will attempt to authenticate using their certificate. If the DC does not support computer account authentication using certificates then authentication with password will be attempted.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

18.9.24 Kernel DMA 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 **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 is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

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).

18.9.26 Local Security Authority

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

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.

18.9.27.1 Ensure 'Disallow copying of user input methods to the system account for sign-in' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy prevents automatic copying of user input methods to the system account for use on the sign-in screen. The user is restricted to the set of input methods that are enabled in the system account.

The recommended state for this setting is: **Enabled**.

Rationale:

This is a way to increase the security of the system account.

Impact:

Users will have input methods enabled for the system account on the sign-in page.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Control  
Panel\International\BlockUserInputMethodsForSignIn
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\System\Locale  
Services\Disallow copying of user input methods to the system account for  
sign-in
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **Globalization.admx/adml** that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (Users will be able to use input methods enabled for their user account on the sign-in page.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

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 Ensure 'Block user from showing account details on sign-in' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy prevents the user from showing account details (email address or user name) on the sign-in screen.

The recommended state for this setting is: **Enabled**.

Rationale:

An attacker with access to the console (for example, someone with physical access or someone who is able to connect to the server through Remote Desktop Services) could view the name of the last user who logged on to the server. The attacker could then try to guess the password, use a dictionary, or use a brute-force attack to try and log on.

Impact:

The user cannot choose to show account details on the sign-in screen.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\System\BlockUserFromShowingAccountDetailsOnSignin
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\System\Logon\Block user from showing account details on sign-in
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **Logon.admx/adml** that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

Default Value:

Disabled. (The user may choose to show account details on the sign-in screen.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

18.9.28.2 Ensure 'Do not display network selection UI' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting allows you to control whether anyone can interact with available networks UI on the logon screen.

The recommended state for this setting is: **Enabled**.

Rationale:

An unauthorized user could disconnect the PC from the network or can connect the PC to other available networks without signing into Windows.

Impact:

The PC's network connectivity state cannot be changed without signing into Windows.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\System:DontDisplayNetworkSelectionUI
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\System\Logon\Do not display network selection UI
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **Logon.admx/adml** that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Disabled. (Any user can disconnect the PC from the network or can connect the PC to other available networks without signing into Windows.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224928
Rule ID: SV-224928r569186_rule
STIG ID: WN16-CC-000180
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

18.9.28.3 Ensure 'Do not enumerate connected users on domain-joined computers' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting prevents connected users from being enumerated on domain-joined computers.

The recommended state for this setting is: **Enabled**.

Rationale:

A malicious user could use this feature to gather account names of other users, that information could then be used in conjunction with other types of attacks such as guessing passwords or social engineering. The value of this countermeasure is small because a user with domain credentials could gather the same account information using other methods.

Impact:

The Logon UI will not enumerate any connected users on domain-joined computers.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\System:DontEnumerateConnectedUsers
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\System\Logon\Do not enumerate connected users on domain-joined computers
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **Logon.admx/adml** that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (Connected users will be enumerated on domain-joined computers.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

18.9.28.4 Ensure 'Enumerate local users on domain-joined computers' is set to 'Disabled' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server
- STIG Member Server

Description:

This policy setting allows local users to be enumerated on domain-joined computers.

The recommended state for this setting is: **Disabled**.

Rationale:

A malicious user could use this feature to gather account names of other users, that information could then be used in conjunction with other types of attacks such as guessing passwords or social engineering. The value of this countermeasure is small because a user with domain credentials could gather the same account information using other methods.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\System:EnumerateLocalUsers
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Administrative  
Templates\System\Logon\Enumerate local users on domain-joined computers
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **Logon.admx/adml** that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (The Logon UI will not enumerate local users on domain-joined computers.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225009
Rule ID: SV-225009r857260_rule
STIG ID: WN16-MS-000030
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

18.9.28.5 Ensure 'Turn off app notifications on the lock screen' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to prevent app notifications from appearing on the lock screen.

The recommended state for this setting is: **Enabled**.

Rationale:

App notifications might display sensitive business or personal data.

Impact:

No app notifications are displayed on the lock screen.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\System:DisableLockScreenAppNotifications
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\System\Logon\Turn off app notifications on the lock screen
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **Logon.admx/adml** that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (Users can choose which apps display notifications on the lock screen.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			

18.9.28.6 Ensure 'Turn off picture password sign-in' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to control whether a domain user can sign in using a picture password.

The recommended state for this setting is: **Enabled**.

Note: If the picture password feature is permitted, the user's domain password is cached in the system vault when using it.

Rationale:

Picture passwords bypass the requirement for a typed complex password. In a shared work environment, a simple shoulder surf where someone observed the on-screen gestures would allow that person to gain access to the system without the need to know the complex password. Vertical monitor screens with an image are much more visible at a distance than horizontal key strokes, increasing the likelihood of a successful observation of the mouse gestures.

Impact:

Users will not be able to set up or sign in with a picture password.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\System:BlockDomainPicturePassword
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\System\Logon\Turn off picture password sign-in
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **CredentialProviders.admx/adml** that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (Users can set up and use a picture password.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			

18.9.28.7 Ensure 'Turn on convenience PIN sign-in' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to control whether a domain user can sign in using a convenience PIN. In Windows 10, convenience PIN was replaced with Passport, which has stronger security properties. To configure Passport for domain users, use the policies under Computer Configuration\Administrative Templates\Windows Components\Microsoft Passport for Work.

Note: The user's domain password will be cached in the system vault when using this feature.

The recommended state for this setting is: **Disabled**.

Rationale:

A PIN is created from a much smaller selection of characters than a password, so in most cases a PIN will be much less robust than a password.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

HKLM\SOFTWARE\Policies\Microsoft\Windows\System:AllowDomainPINLogon

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

Computer Configuration\Policies\Administrative Templates\System\Logon\Turn on convenience PIN sign-in

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **CredentialProviders.admx/adml** that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Turn on PIN sign-in*, but it was renamed starting with the Windows 10 Release 1511 Administrative Templates.

Default Value:

Disabled. (A domain user can't set up and use a convenience PIN.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			

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 is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

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.

18.9.33.6.1 Ensure 'Allow network connectivity during connected-standby (on battery)' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting allows you to control the network connectivity state in standby on modern standby-capable systems.

The recommended state for this setting is: **Disabled**.

Rationale:

Disabling this setting ensures that the computer will not be accessible to attackers over a WLAN network while left unattended, on battery and in a sleep state.

Impact:

Network connectivity in standby (while on battery) is not guaranteed. This connectivity restriction currently only applies to WLAN networks only, but is subject to change (according to Microsoft).

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\Power\PowerSettings\f15576e8-98b7-4186-b944-eafa664402d9:DCSettingIndex
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Administrative Templates\System\Power Management\Sleep Settings\Allow network connectivity during connected-standby (on battery)
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **Power.admx/adml** that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

Default Value:

Enabled. (Network connectivity will be maintained in standby while on battery.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.9.33.6.2 Ensure 'Allow network connectivity during connected-standby (plugged in)' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting allows you to control the network connectivity state in standby on modern standby-capable systems.

The recommended state for this setting is: **Disabled**.

Rationale:

Disabling this setting ensures that the computer will not be accessible to attackers over a WLAN network while left unattended, plugged in and in a sleep state.

Impact:

Network connectivity in standby (while plugged in) is not guaranteed. This connectivity restriction currently only applies to WLAN networks only, but is subject to change (according to Microsoft).

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\Power\PowerSettings\f15576e8-98b7-4186-b944-eafa664402d9:ACSettingIndex
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Administrative Templates\System\Power Management\Sleep Settings\Allow network connectivity during connected-standby (plugged in)
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **Power.admx/adml** that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

Default Value:

Enabled. (Network connectivity will be maintained in standby while plugged in.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.9.33.6.3 Ensure 'Require a password when a computer wakes (on battery)' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

Specifies whether or not the user is prompted for a password when the system resumes from sleep.

The recommended state for this setting is: **Enabled**.

Rationale:

Enabling this setting ensures that anyone who wakes an unattended computer from sleep state will have to provide logon credentials before they can access the system.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Power\PowerSettings\0e796bdb-100d-47d6-a2d5-f7d2daa51f51:DCSettingIndex
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\System\Power Management\Sleep Settings\Require a password when a computer wakes (on battery)
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **Power.admx/adml** that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Enabled. (The user is prompted for a password when the system resumes from sleep while on battery.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224929
Rule ID: SV-224929r569186_rule
STIG ID: WN16-CC-000210
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	16.11 <u>Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

18.9.33.6.4 Ensure 'Require a password when a computer wakes (plugged in)' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

Specifies whether or not the user is prompted for a password when the system resumes from sleep.

The recommended state for this setting is: **Enabled**.

Rationale:

Enabling this setting ensures that anyone who wakes an unattended computer from sleep state will have to provide logon credentials before they can access the system.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Power\PowerSettings\0e796bdb-100d-47d6-a2d5-f7d2daa51f51:ACSettingIndex
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\System\Power Management\Sleep Settings\Require a password when a computer wakes (plugged in)
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **Power.admx/adml** that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Enabled. (The user is prompted for a password when the system resumes from sleep while plugged in.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224930
Rule ID: SV-224930r569186_rule
STIG ID: WN16-CC-000220
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	16.11 <u>Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

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.

18.9.35.1 Ensure 'Configure Offer Remote Assistance' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to turn on or turn off Offer (Unsolicited) Remote Assistance on this computer.

Help desk and support personnel will not be able to proactively offer assistance, although they can still respond to user assistance requests.

The recommended state for this setting is: **Disabled**.

Rationale:

A user might be tricked and accept an unsolicited Remote Assistance offer from a malicious user.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal  
Services:fAllowUnsolicited
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Administrative Templates\System\Remote  
Assistance\Configure Offer Remote Assistance
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **RemoteAssistance.admx/adml** that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (Users on this computer cannot get help from their corporate technical support staff using Offer (Unsolicited) Remote Assistance.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

18.9.35.2 Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to turn on or turn off Solicited (Ask for) Remote Assistance on this computer.

The recommended state for this setting is: **Disabled**.

Rationale:

There is slight risk that a rogue administrator will gain access to another user's desktop session, however, they cannot connect to a user's computer unannounced or control it without permission from the user. When an expert tries to connect, the user can still choose to deny the connection or give the expert view-only privileges. The user must explicitly click the Yes button to allow the expert to remotely control the workstation.

Impact:

Users on this computer cannot use e-mail or file transfer to ask someone for help. Also, users cannot use instant messaging programs to allow connections to this computer.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:fAllowToGetHelp
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Administrative Templates\System\Remote Assistance\Configure Solicited Remote Assistance
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **RemoteAssistance.admx/adml** that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Users can turn on or turn off Solicited (Ask for) Remote Assistance themselves in System Properties in Control Panel. Users can also configure Remote Assistance settings.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

18.9.36 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.

18.9.36.1 Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy setting controls whether RPC clients authenticate with the Endpoint Mapper Service when the call they are making contains authentication information. The Endpoint Mapper Service on computers running Windows NT4 (all service packs) cannot process authentication information supplied in this manner. This policy setting can cause a specific issue with 1-way forest trusts if it is applied to the *trusting* domain DCs (see Microsoft [KB3073942](#)), so we do not recommend applying it to Domain Controllers.

Note: This policy will not be in effect until the system is rebooted.

The recommended state for this setting is: **Enabled**.

Rationale:

Anonymous access to RPC services could result in accidental disclosure of information to unauthenticated users.

Impact:

RPC clients will authenticate to the Endpoint Mapper Service for calls that contain authentication information. Clients making such calls will not be able to communicate with the Windows NT4 Server Endpoint Mapper Service.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Rpc:EnableAuthEpResolution
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\System\Remote Procedure Call\Enable RPC Endpoint Mapper Client Authentication
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **RPC.admx/adml** that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (RPC clients will not authenticate to the Endpoint Mapper Service, but they will be able to communicate with the Windows NT4 Server Endpoint Mapper Service.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.9.36.2 Ensure 'Restrict Unauthenticated RPC clients' is set to 'Enabled: Authenticated' (MS only) (Automated)

Profile Applicability:

- Level 2 - Member Server
- STIG Member Server

Description:

This policy setting controls how the RPC server runtime handles unauthenticated RPC clients connecting to RPC servers.

This policy setting impacts all RPC applications. In a domain environment this policy setting should be used with caution as it can impact a wide range of functionality including group policy processing itself. Reverting a change to this policy setting can require manual intervention on each affected machine. **This policy setting should never be applied to a Domain Controller.**

A client will be considered an authenticated client if it uses a named pipe to communicate with the server or if it uses RPC Security. RPC Interfaces that have specifically requested to be accessible by unauthenticated clients may be exempt from this restriction, depending on the selected value for this policy setting.

- **"None"** allows all RPC clients to connect to RPC Servers running on the machine on which the policy setting is applied.
- **"Authenticated"** allows only authenticated RPC Clients (per the definition above) to connect to RPC Servers running on the machine on which the policy setting is applied. Exemptions are granted to interfaces that have requested them.
- **"Authenticated without exceptions"** allows only authenticated RPC Clients (per the definition above) to connect to RPC Servers running on the machine on which the policy setting is applied. No exceptions are allowed. **This value has the potential to cause serious problems and is not recommended.**

Note: This policy setting will not be applied until the system is rebooted.

The recommended state for this setting is: **Enabled: Authenticated.**

Rationale:

Unauthenticated RPC communication can create a security vulnerability.

Impact:

Only authenticated RPC Clients will be allowed to connect to RPC servers running on the machine on which the policy setting is applied. Exemptions are granted to interfaces that have requested them.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Rpc:RestrictRemoteClients
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled: Authenticated:**

```
Computer Configuration\Policies\Administrative Templates\System\Remote Procedure Call\Restrict Unauthenticated RPC clients
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **RPC.admx/adm1** that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Enabled: None. (All RPC clients are allowed to connect to RPC servers running on the machine.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225010
Rule ID: SV-225010r877039_rule
STIG ID: WN16-MS-000040
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

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.

18.9.47.5.1 Ensure 'Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting configures Microsoft Support Diagnostic Tool (MSDT) interactive communication with the support provider. MSDT gathers diagnostic data for analysis by support professionals.

The recommended state for this setting is: **Disabled**.

Rationale:

Due to privacy concerns, data should never be sent to any third-party since this data could contain sensitive information.

Impact:

MSDT cannot run in support mode, and no data can be collected or sent to the support provider.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\ScriptedDiagnosticsProvider\Policy:DisableQueryRemoteServer
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Administrative Templates\System\Troubleshooting and Diagnostics\Microsoft Support Diagnostic Tool\Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **MSDT.admx/adml** that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Enabled. (Users can use MSDT to collect and send diagnostic data to a support professional to resolve a problem. By default, the support provider is set to Microsoft Corporation.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

18.9.47.6 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).

18.9.47.11.1 Ensure 'Enable/Disable PerfTrack' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting specifies whether to enable or disable tracking of responsiveness events.

The recommended state for this setting is: **Disabled**.

Rationale:

When enabled the aggregated data of a given event will be transmitted to Microsoft. The option exists to restrict this feature for a specific user, set the consent level, and designate specific programs for which error reports could be sent. However, centrally restricting the ability to execute PerfTrack to limit the potential for unauthorized or undesired usage, data leakage, or unintentional communications is highly recommended.

Impact:

Responsiveness events are not processed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\WDI\{9c5a40da-b965-4fc3-8781-88dd50a6299d}:ScenarioExecutionEnabled
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Administrative  
Templates\System\Troubleshooting and Diagnostics\Windows Performance  
PerfTrack\Enable/Disable PerfTrack
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **PerformancePerftrack.admx/adml** that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

Enabled. (Responsiveness events are processed and aggregated. The aggregated data will be transmitted to Microsoft through SQM.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

18.9.48 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.

18.9.49.1 Ensure 'Turn off the advertising ID' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting turns off the advertising ID, preventing apps from using the ID for experiences across apps.

The recommended state for this setting is: **Enabled**.

Rationale:

Tracking user activity for advertising purposes, even anonymously, may be a privacy concern. In an enterprise managed environment, applications should not need or require tracking for targeted advertising.

Impact:

The advertising ID is turned off. Apps can't use the ID for experiences across apps.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\AdvertisingInfo:DisabledByGroupPolicy
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\System\User Profiles\Turn off the advertising ID
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **UserProfiles.admx/adml** that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Disabled. (Users can control whether apps can use the advertising ID for experiences across apps.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

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.

18.9.51.1.1 Ensure 'Enable Windows NTP Client' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting specifies whether the Windows NTP Client is enabled. Enabling the Windows NTP Client allows synchronization from a systems computer clock to NTP server(s).

The recommended state for this setting is: **Enabled**.

Note: If a third-party time provider is used in the environment, an exception to this recommendation will be needed.

Rationale:

A reliable and accurate account of time is important for a number of services and security requirements, including but not limited to distributed applications, authentication services, multi-user databases and logging services. The use of an NTP client (with secure operation) establishes functional accuracy and is a focal point when reviewing security relevant events

Impact:

System time will be synced to the configured NTP server(s).

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\W32Time\TimeProviders\NtpClient:Enabled
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\System\Windows Time Service\Time Providers\Enable Windows NTP Client
```

Note: This Group Policy path is provided by the Group Policy template **W32Time.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (The local computer clock does not synchronize time with NTP servers.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.4 <u>Standardize Time Synchronization</u> Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.			
v7	6.1 <u>Utilize Three Synchronized Time Sources</u> Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.			

18.9.51.1.2 Ensure 'Enable Windows NTP Client' is set to 'Enabled: DoD time server' (STIG only) (Automated)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting specifies whether the Windows NTP Client is enabled. Enabling the Windows NTP Client allows your computer to synchronize its computer clock with other NTP servers. You might want to disable this service if you decide to use a third-party time provider.

The recommended STIG state for this setting is: **Enabled** and configure the *NtpServer* field to **Point to an appropriate DoD time server**.

Rationale:

A reliable and accurate account of time is important for a number of services and security requirements, including but not limited to distributed applications, authentication services, multi-user databases and logging services. The use of an NTP client (with secure operation) establishes functional accuracy and is a focal point when reviewing security relevant events

Impact:

You can set the local computer clock to synchronize time with NTP servers.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\W32Time\TimeProviders\NtpClient:Enabled
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\System\Windows Time Service\Time Providers\Enable Windows NTP Client
```

Note: This Group Policy path is provided by the Group Policy template **W32Time.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (The local computer clock does not synchronize time with NTP servers.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224862
Rule ID: SV-224862r921955_rule
STIG ID: WN16-00-000450
Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.4 Standardize Time Synchronization Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.			
v7	6.1 Utilize Three Synchronized Time Sources Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.			

18.9.51.1.3 Ensure 'Enable Windows NTP Server' is set to 'Disabled' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy setting specifies whether the Windows NTP Server is enabled. Disabling this setting prevents the system from acting as a NTP Server (time source) to service NTP requests from other systems (NTP Clients).

The recommended state for this setting is: **Disabled**.

Note: In most enterprise managed environments, you should *not* disable the Windows NTP Server on Domain Controllers, as it is very important for the operation of NT5DS (domain hierarchy-based) time synchronization.

Rationale:

The configuration of proper time synchronization is critically important in an enterprise managed environment both due to the sensitivity of Kerberos authentication timestamps and also to ensure accurate security logging. This should be done through a known NTP server. Member servers and workstations should not typically be time sources for other clients.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\W32Time\TimeProviders\NtpServer:Enabled
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Administrative Templates\System\Windows Time Service\Time Providers\Enable Windows NTP Server
```

Note: This Group Policy path is provided by the Group Policy template **W32Time.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (The computer cannot service NTP requests from other computers.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.4 <u>Standardize Time Synchronization</u> Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.			
v7	6.1 <u>Utilize Three Synchronized Time Sources</u> Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.			

18.10 Windows Components

This section contains recommendations for Windows Component settings.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.1 ActiveX Installer Service

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `ActiveXInstallService.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.2 Add features to Windows 10 (formerly Windows Anytime Upgrade)

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsAnytimeUpgrade.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Note: This section was initially named *Windows Anytime Upgrade* but was renamed by Microsoft to *Add features to Windows x* starting with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

18.10.3 App 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).

18.10.3.1 Ensure 'Allow a Windows app to share application data between users' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

Manages a Windows app's ability to share data between users who have installed the app. Data is shared through the **SharedLocal** folder. This folder is available through the **Windows.Storage** API.

The recommended state for this setting is: **Disabled**.

Rationale:

Users of a system could accidentally share sensitive data with other users on the same system.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\AppModel\StateManager  
:AllowSharedLocalAppData
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\App Package Deployment\Allow a Windows app to share application  
data between users
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **AppxPackageManager.admx/adml** that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

Default Value:

Disabled. (Windows apps won't be able to share app data with other instances of that app.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	14.6 <u>Protect Information through Access Control Lists</u> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

18.10.4 App Privacy

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template [AppPrivacy.admx/adml](#) that is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).

18.10.5 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).

18.10.5.1 Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting lets you control whether Microsoft accounts are optional for Windows Store apps that require an account to sign in. This policy only affects Windows Store apps that support it.

The recommended state for this setting is: **Enabled**.

Rationale:

Enabling this setting allows an organization to use their enterprise user accounts instead of using their Microsoft accounts when accessing Windows store apps. This provides the organization with greater control over relevant credentials. Microsoft accounts cannot be centrally managed and as such enterprise credential security policies cannot be applied to them, which could put any information accessed by using Microsoft accounts at risk.

Impact:

Windows Store apps that typically require a Microsoft account to sign in will allow users to sign in with an enterprise account instead.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:MSAOptional
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\App runtime\Allow Microsoft accounts to be optional
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **AppXRuntime.admx/adml** that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Disabled. (Users will need to sign in with a Microsoft account.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.6 <u>Centralize Account Management</u> Centralize account management through a directory or identity service.			
v7	16.2 <u>Configure Centralized Point of Authentication</u> Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.			

18.10.6 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.

18.10.6.1 Ensure 'Turn off Inventory Collector' is set to 'Enabled' (STIG only) (Automated)

Profile Applicability:

- STIG Member Server
- STIG Domain Controller

Description:

This policy setting inventories applications, files, devices, and drivers on the system and sends the information to Microsoft. This information is used to help diagnose compatibility problems.

The STIG recommended state for this setting is: **Enabled**.

Rationale:

Sending data to a 3rd party vendor is a security concern and should only be done on an as needed basis.

Impact:

Applications, files, devices, and drivers inventories will not be sent to Microsoft.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\AppCompat:DisableInventory
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Application Compatibility\Turn off Inventory Collector
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **AppCompat.admx/adml** that is included with the Microsoft Windows 7 & Server 2008R2 Administrative Templates (or newer).

Default Value:

Enabled - If this policy setting is enabled or not configured, the inventory collector will be turned on.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224931
Rule ID: SV-224931r569186_rule
STIG ID: WN16-CC-000240
Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

18.10.7 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.

18.10.7.1 Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting disallows AutoPlay for MTP devices like cameras or phones.

The recommended state for this setting is: **Enabled**.

Rationale:

An attacker could use this feature to launch a program to damage a client computer or data on the computer.

Impact:

AutoPlay will not be allowed for MTP devices like cameras or phones.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Explorer:NoAutoplayfornonVolume
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\AutoPlay Policies\Disallow Autoplay for non-volume devices
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **AutoPlay.admx/adml** that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (AutoPlay is enabled for non-volume devices.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224932
Rule ID: SV-224932r852325_rule
STIG ID: WN16-CC-000250
Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>10.3 Disable Autorun and Autoplay for Removable Media</u> Disable autorun and autoplay auto-execute functionality for removable media.			
v7	<u>8.5 Configure Devices Not To Auto-run Content</u> Configure devices to not auto-run content from removable media.			

18.10.7.2 Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting sets the default behavior for Autorun commands. Autorun commands are generally stored in **autorun.inf** files. They often launch the installation program or other routines.

The recommended state for this setting is: **Enabled: Do not execute any autorun commands**.

Rationale:

Prior to Windows Vista, when media containing an autorun command is inserted, the system will automatically execute the program without user intervention. This creates a major security concern as code may be executed without user's knowledge. The default behavior starting with Windows Vista is to prompt the user whether autorun command is to be run. The autorun command is represented as a handler in the Autoplay dialog.

Impact:

AutoRun commands will be completely disabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer:NoAutorun
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled: Do not execute any autorun commands:**

```
Computer Configuration\Policies\Administrative Templates\Windows Components\AutoPlay Policies\Set the default behavior for AutoRun
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **AutoPlay.admx/adml** that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (Windows will prompt the user whether autorun command is to be run.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224933
Rule ID: SV-224933r852326_rule
STIG ID: WN16-CC-000260
Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.3 <u>Disable Autorun and Autoplay for Removable Media</u> Disable autorun and autoplay auto-execute functionality for removable media.			
v7	8.5 <u>Configure Devices Not To Auto-run Content</u> Configure devices to not auto-run content from removable media.			

18.10.7.3 Ensure 'Turn off Autoplay' is set to 'Enabled: All drives' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

Autoplay starts to read from a drive as soon as you insert media in the drive, which causes the setup file for programs or audio media to start immediately. An attacker could use this feature to launch a program to damage the computer or data on the computer. Autoplay is disabled by default on some removable drive types, such as floppy disk and network drives, but not on CD-ROM drives.

Note: You cannot use this policy setting to enable Autoplay on computer drives in which it is disabled by default, such as floppy disk and network drives.

The recommended state for this setting is: **Enabled: All drives**.

Rationale:

An attacker could use this feature to launch a program to damage a client computer or data on the computer.

Impact:

Autoplay will be disabled - users will have to manually launch setup or installation programs that are provided on removable media.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **255**.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer:NoDriveTypeAutoRun
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled: All drives**:

Computer Configuration\Policies\Administrative Templates\Windows Components\AutoPlay Policies\Turn off Autoplay

Note: This Group Policy path is provided by the Group Policy template **AutoPlay.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Autoplay is enabled.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224934
Rule ID: SV-224934r852327_rule
STIG ID: WN16-CC-000270
Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>10.3 Disable Autorun and Autoplay for Removable Media</u> Disable autorun and autoplay auto-execute functionality for removable media.			
v7	<u>8.5 Configure Devices Not To Auto-run Content</u> Configure devices to not auto-run content from removable media.			

18.10.8 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).

18.10.8.1 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).

18.10.8.1.1 Ensure 'Configure enhanced anti-spoofing' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether enhanced anti-spoofing is configured for devices which support it.

The recommended state for this setting is: **Enabled**.

Rationale:

Enterprise managed environments are now supporting a wider range of mobile devices, increasing the security on these devices will help protect against unauthorized access on your network.

Impact:

Windows will require all users on the device to use anti-spoofing for facial features, on devices which support it.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Biometrics\FacialFeatures:EnhancedAntiSpoofing
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Biometrics\Facial Features\Configure enhanced anti-spoofing
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **Biometrics.admx/adml** that is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).

Note #2: In the Windows 10 Release 1511 and Windows 10 Release 1607 & Server 2016 Administrative Templates, this setting was initially named *Use enhanced anti-spoofing when available*. It was renamed to *Configure enhanced anti-spoofing* starting with the Windows 10 Release 1703 Administrative Templates.

Default Value:

Users are able to choose whether or not to use enhanced anti-spoofing on supported devices.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

18.10.9 BitLocker Drive Encryption

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template [VolumeEncryption.admx/adml](#) that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.10 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).

18.10.10.1 Ensure 'Allow Use of Camera' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting controls whether the use of Camera devices on the machine are permitted.

The recommended state for this setting is: **Disabled**.

Rationale:

Cameras in a high security environment can pose serious privacy and data exfiltration risks - they should be disabled to help mitigate that risk.

Impact:

Users will not be able to utilize the camera on a system.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\Camera:AllowCamera
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Camera\Allow Use of Camera
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **Camera.admx/adml** that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

Default Value:

Enabled. (Camera devices are enabled.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			

18.10.11 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).

18.10.12 Cloud Content

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

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).

18.10.12.1 Ensure 'Turn off cloud consumer account state content' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether cloud consumer account state content is allowed in all Windows experiences.

The recommended state for this setting is: **Enabled**.

Rationale:

The use of consumer accounts in an enterprise managed environment is not good security practice as it could lead to possible data leakage.

Impact:

Users will not be able to use Microsoft consumer accounts on the system, and associated Windows experiences will instead present default fallback content.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\CloudContent:DisableConsumerAccountStateContent
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Cloud Content\Turn off cloud consumer account state content
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **CloudContent.admx/adml** that is included with the Microsoft Windows 11 Release 21H2 Administrative Templates (or newer).

Default Value:

Disabled. (Windows experiences are able to use cloud consumer accounts.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.6 <u>Centralize Account Management</u> Centralize account management through a directory or identity service.			

18.10.12.2 Ensure 'Turn off Microsoft consumer experiences' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting turns off experiences that help consumers make the most of their devices and Microsoft account.

The recommended state for this setting is: **Enabled**.

Note: [Per Microsoft TechNet](#), this policy setting only applies to Windows 10 Enterprise and Windows 10 Education editions.

Rationale:

Having apps silently install in an enterprise managed environment is not good security practice - especially if the apps send data back to a third-party.

Impact:

Users will no longer see personalized recommendations from Microsoft and notifications about their Microsoft account.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\CloudContent:DisableWindowsConsumerFeatures
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Cloud Content\Turn off Microsoft consumer experiences
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **CloudContent.admx/adml** that is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).

Default Value:

Disabled. (Users may see suggestions from Microsoft and notifications about their Microsoft account.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

18.10.13 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).

18.10.13.1 Ensure 'Require pin for pairing' is set to 'Enabled: First Time' OR 'Enabled: Always' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls whether or not a PIN is required for pairing to a wireless display device.

The recommended state for this setting is: **Enabled: First Time** OR **Enabled: Always**.

Rationale:

If this setting is not configured or disabled then a PIN would not be required when pairing wireless display devices to the system, increasing the risk of unauthorized use.

Impact:

The pairing ceremony for connecting to new wireless display devices will always require a PIN.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1** or **2**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Connect:RequirePinForPairing
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled: First Time** OR **Enabled: Always**:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Connect\Require pin for pairing
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **WirelessDisplay.admx/adml** that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer). The new **Choose one of the following actions** sub-option was later added as of the Windows 10 Release 1809 Administrative Templates. Choosing **Enabled** in the older templates is the equivalent of choosing **Enabled: First Time** in the newer templates.

Default Value:

Disabled. (A PIN is not required for pairing to a wireless display device.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

18.10.14 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.

18.10.14.1 Ensure 'Do not display the password reveal button' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to configure the display of the password reveal button in password entry user experiences.

The recommended state for this setting is: **Enabled**.

Rationale:

This is a useful feature when entering a long and complex password, especially when using a touchscreen. The potential risk is that someone else may see your password while surreptitiously observing your screen.

Impact:

The password reveal button will not be displayed after a user types a password in the password entry text box.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\CredUI:DisablePasswordReveal
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Credential User Interface\Do not display the password reveal  
button
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **CredUI.admx/adml** that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (The password reveal button is displayed after a user types a password in the password entry text box. If the user clicks on the button, the typed password is displayed on-screen in plain text.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

18.10.14.2 Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting controls whether administrator accounts are displayed when a user attempts to elevate a running application.

The recommended state for this setting is: **Disabled**.

Rationale:

Users could see the list of administrator accounts, making it slightly easier for a malicious user who has logged onto a console session to try to crack the passwords of those accounts.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\CredUI:EnumerateAdministrators
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Credential User Interface\Enumerate administrator accounts on elevation
```

Note: This Group Policy path is provided by the Group Policy template **CredUI.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Users will be required to always type in a username and password to elevate.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224935
Rule ID: SV-224935r569186_rule
STIG ID: WN16-CC-000280
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

18.10.15 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).

18.10.15.1 Ensure 'Allow Diagnostic Data' is set to 'Enabled: Diagnostic data off (not recommended)' or 'Enabled: Send required diagnostic data' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting determines the amount of diagnostic and usage data reported to Microsoft:

- A value of (0) **Diagnostic data off (not recommended)**. Using this value, no diagnostic data is sent from the device. This value is only supported on Enterprise, Education, and Server editions. If you choose this setting, devices in your organization will still be secure.
- A value of (1) **Send required diagnostic data**. This is the minimum diagnostic data necessary to keep Windows secure, up to date, and performing as expected. Using this value disables the *Optional diagnostic data* control in the Settings app.
- A value of (3) **Send optional diagnostic data**. Additional diagnostic data is collected that helps us to detect, diagnose and fix issues, as well as make product improvements. Required diagnostic data will always be included when you choose to send optional diagnostic data. Optional diagnostic data can also include diagnostic log files and crash dumps. Use the *Limit Dump Collection* and the *Limit Diagnostic Log Collection* policies for more granular control of what optional diagnostic data is sent.

Windows telemetry settings apply to the Windows operating system and some first party apps. This setting does not apply to third party apps running on Windows 10/11.

The recommended state for this setting is: **Enabled: Diagnostic data off (not recommended)** or **Enabled: Send required diagnostic data**.

Note: If your organization relies on Windows Update, the minimum recommended setting is **Required diagnostic data**. Because no Windows Update information is collected when diagnostic data is off, important information about update failures is not sent. Microsoft uses this information to fix the causes of those failures and improve the quality of updates.

Note #2: The *Configure diagnostic data opt-in settings user interface* group policy can be used to prevent end users from changing their data collection settings.

Note #3: Enhanced diagnostic data setting is not available on Windows 11 and Windows Server 2022 and has been replaced with policies that can control the amount of optional diagnostic data that is sent. For more information on these settings visit [Manage diagnostic data using Group Policy and MDM](#)

Rationale:

Sending any data to a third-party vendor is a security concern and should only be done on an as needed basis.

Impact:

Note that setting values of 0 or 1 will degrade certain experiences on the device.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0** or **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\DataCollection:AllowTelemetry
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled: Diagnostic data off (not recommended)** or **Enabled: Send required diagnostic data**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Data Collection and Preview Builds\Allow Diagnostic Data
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **DataCollection.admx/adml** that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Allow Telemetry*, but it was renamed to *Allow Diagnostic Data* starting with the Windows 11 Release 21H2 Administrative Templates.

Default Value:

Disabled. (The device will send required diagnostic data and the end user can choose whether to send optional diagnostic data from the Settings app.)

References:

1. <https://docs.microsoft.com/en-us/windows/privacy/configure-windows-diagnostic-data-in-your-organization>

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224936
Rule ID: SV-224936r569186_rule
STIG ID: WN16-CC-000290
Severity: CAT II

Note: The Microsoft Windows Server 2016 Security Technical Implementation Guide (STIG) refers to the older setting, *Allow Telemetry*, and not the newer setting as described in this recommendation. The STIG allowed configuration state is either **0 - Security [Enterprise Only]** or **1 - Basic** which translates to the newer options of **Enabled: Diagnostic data off (not recommended)** or **Enabled: Send required diagnostic data**. Setting this to the CIS recommended state should conform to the STIG.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.10.15.2 Ensure 'Configure Authenticated Proxy usage for the Connected User Experience and Telemetry service' is set to 'Enabled: Disable Authenticated Proxy usage' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting controls whether the Connected User Experience and Telemetry service can automatically use an authenticated proxy to send data back to Microsoft.

The recommended state for this setting is: **Enabled: Disable Authenticated Proxy usage**.

Rationale:

Sending any data to a third-party vendor is a security concern and should only be done on an as needed basis.

Impact:

The Connected User Experience and Telemetry service will be blocked from automatically using an authenticated proxy.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\DataCollection:DisableEnterpriseAuthProxy
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled: Disable Authenticated Proxy usage**:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Data Collection and Preview Builds\Configure Authenticated Proxy usage for the Connected User Experience and Telemetry service
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **DataCollection.admx/adml** that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

Default Value:

Disabled. (The Connected User Experience and Telemetry service will automatically use an authenticated proxy to send data back to Microsoft.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

18.10.15.3 Ensure 'Disable OneSettings Downloads' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls whether Windows attempts to connect with the OneSettings service to download configuration settings.

The recommended state for this setting is: **Enabled**.

Rationale:

Sending data to a third-party vendor is a security concern and should only be done on an as-needed basis.

Impact:

Windows will not connect to the OneSettings service to download configuration settings.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\DataCollection:DisableOneSettingsDownloads
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Data Collection and Preview Builds\Disable OneSettings Downloads
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **DataCollection.admx/adml** that is included with the Microsoft Windows 11 Release 21H2 Administrative Templates (or newer).

Default Value:

Disabled. (Windows will periodically attempt to connect with the OneSettings service to download configuration settings.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

18.10.15.4 Ensure 'Do not show feedback notifications' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows an organization to prevent its devices from showing feedback questions from Microsoft.

The recommended state for this setting is: **Enabled**.

Rationale:

Users should not be sending any feedback to third-party vendors in an enterprise managed environment.

Impact:

Users will no longer see feedback notifications through the Windows Feedback app.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\DataCollection:DoNotShowFeedbackNotifications
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Data Collection and Preview Builds\Do not show feedback notifications
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **FeedbackNotifications.admx/adml** that is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).

Default Value:

Disabled. (Users may see notifications through the Windows Feedback app asking users for feedback. Users can control how often they receive feedback questions.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.10.15.5 Ensure 'Enable OneSettings Auditing' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls whether Windows records attempts to connect with the OneSettings service to the Event Log.

The recommended state for this setting is: **Enabled**.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Impact:

Windows will record attempts to connect with the OneSettings service to the **Applications and Services Logs\Microsoft\Windows\Privacy-Auditing\Operational** Event Log channel.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\DataCollection:EnableOneSettingsAuditing
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Data Collection and Preview Builds\Enable OneSettings Auditing
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **DataCollection.admx/adml** that is included with the Microsoft Windows 11 Release 21H2 Administrative Templates (or newer).

Default Value:

Disabled. (Windows will not record attempts to connect with the OneSettings service to the Event Log.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	8.5 <u>Configure Devices Not To Auto-run Content</u> Configure devices to not auto-run content from removable media.			

18.10.15.6 Ensure 'Limit Diagnostic Log Collection' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls whether additional diagnostic logs are collected when more information is needed to troubleshoot a problem on the device.

The recommended state for this setting is: **Enabled**.

Note: Diagnostic logs are only sent when the device has been configured to send optional diagnostic data. Diagnostic data is limited when recommendation **Allow Diagnostic Data** is set to **Enabled: Diagnostic data off (not recommended)** or **Enabled: Send required diagnostic data** to send only basic information.

Rationale:

Sending data to a third-party vendor is a security concern and should only be done on an as-needed basis.

Impact:

Diagnostic logs and information such as crash dumps will not be collected for transmission to Microsoft.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\DataCollection:LimitDiagnosticLogCollection
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Data Collection and Preview Builds\Limit Diagnostic Log Collection
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **DataCollection.admx/adml** that is included with the Microsoft Windows 11 Release 21H2 Administrative Templates (or newer).

Default Value:

Disabled. (Microsoft may occasionally collect diagnostic logs if the device has been configured to send optional diagnostic data.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			

18.10.15.7 Ensure 'Limit Dump Collection' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting limits the type of memory dumps that can be collected when more information is needed to troubleshoot a problem.

The recommended state for this setting is: **Enabled**.

Note: Memory dumps are only sent when the device has been configured to send optional diagnostic data. Diagnostic data is limited when recommendation **Allow Diagnostic Data** is set to **Enabled: Diagnostic data off (not recommended)** or **Enabled: Send required diagnostic data** to send only basic information.

Rationale:

Memory dumps can contain sensitive information - sending such data to a third-party vendor is a security concern and should only be done on an as-needed basis.

Impact:

Windows Error Reporting will not send full and/or heap memory dumps to Microsoft - they will be limited to kernel mini and/or user mode triage memory dumps (if sending optional diagnostic data is permitted).

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\DataCollection:LimitDumpCollection
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**.

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Data Collection and Preview Builds\Limit Dump Collection
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **DataCollection.admx/adml** that is included with the Microsoft Windows 11 Release 21H2 Administrative Templates (or newer).

Default Value:

Disabled. (Microsoft may occasionally collect full or heap memory dumps, if sending optional diagnostic data is permitted.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

18.10.15.8 Ensure 'Toggle user control over Insider builds' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether users can access the Insider build controls in the Advanced Options for Windows Update. These controls are located under "Get Insider builds," and enable users to make their devices available for downloading and installing Windows preview software.

The recommended state for this setting is: **Disabled**.

Note: This policy setting applies only to devices running Windows Server 2016, up until Release 1703. For Release 1709 or newer, Microsoft encourages using the **Manage preview builds** setting (recommendation title 'Manage preview builds'). We have kept this setting in the benchmark to ensure that any older builds of Windows Server 2016 in the environment are still enforced.

Rationale:

It can be risky for experimental features to be allowed in an enterprise managed environment because this can introduce bugs and security holes into systems, making it easier for an attacker to gain access. It is generally preferred to only use production-ready builds.

Impact:

The item "Get Insider builds" will be unavailable.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

HKLM\SOFTWARE\Policies\Microsoft\Windows\PreviewBuilds:AllowBuildPreview

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

Computer Configuration\Policies\Administrative Templates\Windows Components\Data Collection and Preview Builds\Toggle user control over Insider builds

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **AllowBuildPreview.admx/adml** that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

Default Value:

Enabled. (Users can download and install Windows preview software on their devices.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.3 <u>Address Unauthorized Software</u> Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.			
v7	2.6 <u>Address unapproved software</u> Ensure that unauthorized software is either removed or the inventory is updated in a timely manner			

18.10.16 Delivery Optimization

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template **DeliveryOptimization.admx/adml** that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

18.10.17 Desktop App Installer

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template **DesktopAppInstaller.admx/adml** that is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v1.0 (or newer).

18.10.18 Desktop Gadgets

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template **Sidebar.admx/adml** that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.10.19 Desktop Window Manager

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template **DWM.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.20 Device and Driver Compatibility

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template **DeviceCompat.admx/adml** that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.10.21 Device Registration (formerly Workplace Join)

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template [WorkplaceJoin.admx/adml](#) that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Note: This section was initially named *Workplace Join* but was renamed by Microsoft to *Device Registration* starting with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates.

18.10.22 Digital Locker

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template [DigitalLocker.admx/adml](#) that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.23 Edge UI

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template [EdgeUI.admx/adml](#) that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.10.24 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).

18.10.25 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.

18.10.25.1 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.

18.10.25.1.1 Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls Event Log behavior when the log file reaches its maximum size.

The recommended state for this setting is: **Disabled**.

Note: Old events may or may not be retained according to the *Backup log automatically when full* policy setting.

Rationale:

If new events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_SZ** value of **0**.

HKLM\SOFTWARE\Policies\Microsoft\Windows\EventLog\Application:Retention

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Event Log Service\Application\Control Event Log behavior when the  
log file reaches its maximum size
```

Note: This Group Policy path is provided by the Group Policy template **EventLog.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Retain old events*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Default Value:

Disabled. (When a log file reaches its maximum size, new events overwrite old events.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 <u>Ensure Adequate Audit Log Storage</u> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●
v7	6.4 <u>Ensure adequate storage for logs</u> Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

18.10.25.1.2 Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting specifies the maximum size of the log file in kilobytes. The maximum log file size can be configured between 1 megabyte (1,024 kilobytes) and 4 terabytes (4,194,240 kilobytes) in kilobyte increments.

The recommended state for this setting is: **Enabled: 32,768 or greater**.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Impact:

When event logs fill to capacity, they will stop recording information unless the retention method for each is set so that the computer will overwrite the oldest entries with the most recent ones. To mitigate the risk of loss of recent data, you can configure the retention method so that older events are overwritten as needed.

The consequence of this configuration is that older events will be removed from the logs. Attackers can take advantage of such a configuration, because they can generate a large number of extraneous events to overwrite any evidence of their attack. These risks can be somewhat reduced if you automate the archival and backup of event log data.

Ideally, all specifically monitored events should be sent to a server that uses Microsoft System Center Operations Manager (SCOM) or some other automated monitoring tool. Such a configuration is particularly important because an attacker who successfully compromises a server could clear the Security log. If all events are sent to a monitoring server, then you will be able to gather forensic information about the attacker's activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **32768**.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\EventLog\Application:MaxSize
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled: 32,768 or greater**:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Application\Specify the maximum log file size (KB)
```

Note: This Group Policy path is provided by the Group Policy template **EventLog.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Maximum Log Size (KB)*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Default Value:

Disabled. (The default log size is 20,480 KB - this value can be changed by the local administrator using the Log Properties dialog.)

Additional Information:

```
Microsoft Windows Server 2016 Security Technical Implementation Guide:  
Version 2, Release 8, Benchmark Date: May 15, 2024
```

```
Vul ID: V-224937  
Rule ID: SV-224937r877391_rule  
STIG ID: WN16-CC-000300  
Severity: CAT II
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 <u>Ensure Adequate Audit Log Storage</u> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.			
v7	6.4 <u>Ensure adequate storage for logs</u> Ensure that all systems that store logs have adequate storage space for the logs generated.			

18.10.25.2 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.

18.10.25.2.1 Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls Event Log behavior when the log file reaches its maximum size.

The recommended state for this setting is: **Disabled**.

Note: Old events may or may not be retained according to the *Backup log automatically when full* policy setting.

Rationale:

If new events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_SZ** value of **0**.

HKLM\SOFTWARE\Policies\Microsoft\Windows\EventLog\Security:Retention

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Event Log Service\Security\Control Event Log behavior when the log  
file reaches its maximum size
```

Note: This Group Policy path is provided by the Group Policy template **EventLog.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Retain old events*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Default Value:

Disabled. (When a log file reaches its maximum size, new events overwrite old events.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 <u>Ensure Adequate Audit Log Storage</u> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.			
v7	6.4 <u>Ensure adequate storage for logs</u> Ensure that all systems that store logs have adequate storage space for the logs generated.			

18.10.25.2.2 Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting specifies the maximum size of the log file in kilobytes. The maximum log file size can be configured between 1 megabyte (1,024 kilobytes) and 4 terabytes (4,194,240 kilobytes) in kilobyte increments.

The recommended state for this setting is: **Enabled: 196,608 or greater.**

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Impact:

When event logs fill to capacity, they will stop recording information unless the retention method for each is set so that the computer will overwrite the oldest entries with the most recent ones. To mitigate the risk of loss of recent data, you can configure the retention method so that older events are overwritten as needed.

The consequence of this configuration is that older events will be removed from the logs. Attackers can take advantage of such a configuration, because they can generate a large number of extraneous events to overwrite any evidence of their attack. These risks can be somewhat reduced if you automate the archival and backup of event log data.

Ideally, all specifically monitored events should be sent to a server that uses Microsoft System Center Operations Manager (SCOM) or some other automated monitoring tool. Such a configuration is particularly important because an attacker who successfully compromises a server could clear the Security log. If all events are sent to a monitoring server, then you will be able to gather forensic information about the attacker's activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **196608**.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\EventLog\Security:MaxSize
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled: 196,608 or greater**:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Security\Specify the maximum log file size (KB)
```

Note: This Group Policy path is provided by the Group Policy template **EventLog.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Maximum Log Size (KB)*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Default Value:

Disabled. (The default log size is 20,480 KB - this value can be changed by the local administrator using the Log Properties dialog.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224938
Rule ID: SV-224938r877391_rule
STIG ID: WN16-CC-000310
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 <u>Ensure Adequate Audit Log Storage</u> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●
v7	6.4 <u>Ensure adequate storage for logs</u> Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

18.10.25.3 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.

18.10.25.3.1 Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls Event Log behavior when the log file reaches its maximum size.

The recommended state for this setting is: **Disabled**.

Note: Old events may or may not be retained according to the *Backup log automatically when full* policy setting.

Rationale:

If new events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_SZ** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\EventLog\Setup:Retention
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Event Log Service\Setup\Control Event Log behavior when the log  
file reaches its maximum size
```

Note: This Group Policy path is provided by the Group Policy template **EventLog.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Retain old events*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Default Value:

Disabled. (When a log file reaches its maximum size, new events overwrite old events.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 <u>Ensure Adequate Audit Log Storage</u> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.			
v7	6.4 <u>Ensure adequate storage for logs</u> Ensure that all systems that store logs have adequate storage space for the logs generated.			

18.10.25.3.2 Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting specifies the maximum size of the log file in kilobytes. The maximum log file size can be configured between 1 megabyte (1,024 kilobytes) and 4 terabytes (4,194,240 kilobytes) in kilobyte increments.

The recommended state for this setting is: **Enabled: 32,768 or greater**.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users

Impact:

When event logs fill to capacity, they will stop recording information unless the retention method for each is set so that the computer will overwrite the oldest entries with the most recent ones. To mitigate the risk of loss of recent data, you can configure the retention method so that older events are overwritten as needed.

The consequence of this configuration is that older events will be removed from the logs. Attackers can take advantage of such a configuration, because they can generate a large number of extraneous events to overwrite any evidence of their attack. These risks can be somewhat reduced if you automate the archival and backup of event log data.

Ideally, all specifically monitored events should be sent to a server that uses Microsoft System Center Operations Manager (SCOM) or some other automated monitoring tool. Such a configuration is particularly important because an attacker who successfully compromises a server could clear the Security log. If all events are sent to a monitoring server, then you will be able to gather forensic information about the attacker's activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **32768**.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\EventLog\Setup:MaxSize

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled: 32,768 or greater**:

Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Setup\Specify the maximum log file size (KB)

Note: This Group Policy path is provided by the Group Policy template **EventLog.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Maximum Log Size (KB)*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Default Value:

Disabled. (The default log size is 20,480 KB - this value can be changed by the local administrator using the Log Properties dialog.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 <u>Ensure Adequate Audit Log Storage</u> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.			
v7	6.4 <u>Ensure adequate storage for logs</u> Ensure that all systems that store logs have adequate storage space for the logs generated.			

18.10.25.4 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.

18.10.25.4.1 Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls Event Log behavior when the log file reaches its maximum size.

The recommended state for this setting is: **Disabled**.

Note: Old events may or may not be retained according to the *Backup log automatically when full* policy setting.

Rationale:

If new events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_SZ** value of **0**.

HKLM\SOFTWARE\Policies\Microsoft\Windows\EventLog\System:Retention

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Event Log Service\System\Control Event Log behavior when the log  
file reaches its maximum size
```

Note: This Group Policy path is provided by the Group Policy template **EventLog.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Retain old events*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Default Value:

Disabled. (When a log file reaches its maximum size, new events overwrite old events.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 <u>Ensure Adequate Audit Log Storage</u> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.			
v7	6.4 <u>Ensure adequate storage for logs</u> Ensure that all systems that store logs have adequate storage space for the logs generated.			

18.10.25.4.2 Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting specifies the maximum size of the log file in kilobytes. The maximum log file size can be configured between 1 megabyte (1,024 kilobytes) and 4 terabytes (4,194,240 kilobytes) in kilobyte increments.

The recommended state for this setting is: **Enabled: 32,768 or greater**.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users

Impact:

When event logs fill to capacity, they will stop recording information unless the retention method for each is set so that the computer will overwrite the oldest entries with the most recent ones. To mitigate the risk of loss of recent data, you can configure the retention method so that older events are overwritten as needed.

The consequence of this configuration is that older events will be removed from the logs. Attackers can take advantage of such a configuration, because they can generate a large number of extraneous events to overwrite any evidence of their attack. These risks can be somewhat reduced if you automate the archival and backup of event log data.

Ideally, all specifically monitored events should be sent to a server that uses Microsoft System Center Operations Manager (SCOM) or some other automated monitoring tool. Such a configuration is particularly important because an attacker who successfully compromises a server could clear the Security log. If all events are sent to a monitoring server, then you will be able to gather forensic information about the attacker's activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **32768**.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\EventLog\System:MaxSize
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled: 32,768 or greater**:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\System\Specify the maximum log file size (KB)
```

Note: This Group Policy path is provided by the Group Policy template **EventLog.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Maximum Log Size (KB)*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Default Value:

Disabled. (The default log size is 20,480 KB - this value can be changed by the local administrator using the Log Properties dialog.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224939
Rule ID: SV-224939r877391_rule
STIG ID: WN16-CC-000320
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 <u>Ensure Adequate Audit Log Storage</u> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●
v7	6.4 <u>Ensure adequate storage for logs</u> Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

18.10.26 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).

18.10.27 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.

18.10.28 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.

18.10.28.1 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.

18.10.28.2 Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

Disabling Data Execution Prevention can allow certain legacy plug-in applications to function without terminating Explorer.

The recommended state for this setting is: **Disabled**.

Note: Some legacy plug-in applications and other software may not function with Data Execution Prevention and will require an exception to be defined for that specific plug-in/software.

Rationale:

Data Execution Prevention is an important security feature supported by Explorer that helps to limit the impact of certain types of malware.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Explorer:NoDataExecutionPrevention
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\File Explorer\Turn off Data Execution Prevention for Explorer
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **Explorer.admx/adml** that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

Disabled. (Data Execution Prevention will block certain types of malware from exploiting Explorer.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224941
Rule ID: SV-224941r852331_rule
STIG ID: WN16-CC-000340
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 <u>Enable Anti-Exploitation Features</u> Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 <u>Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies</u> Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

18.10.28.3 Ensure 'Turn off heap termination on corruption' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

Without heap termination on corruption, legacy plug-in applications may continue to function when a File Explorer session has become corrupt. Ensuring that heap termination on corruption is active will prevent this.

The recommended state for this setting is: **Disabled**.

Rationale:

Allowing an application to function after its session has become corrupt increases the risk posture to the system.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Explorer:NoHeapTerminationOnCorruption
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\File Explorer\Turn off heap termination on corruption
```

Note: This Group Policy path is provided by the Group Policy template **Explorer.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Heap termination on corruption is enabled.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224942
Rule ID: SV-224942r569186_rule
STIG ID: WN16-CC-000350
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<u>8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies</u> Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

18.10.28.4 Ensure 'Turn off shell protocol protected mode' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting allows you to configure the amount of functionality that the shell protocol can have. When using the full functionality of this protocol, applications can open folders and launch files. The protected mode reduces the functionality of this protocol allowing applications to only open a limited set of folders. Applications are not able to open files with this protocol when it is in the protected mode. It is recommended to leave this protocol in the protected mode to increase the security of Windows.

The recommended state for this setting is: **Disabled**.

Rationale:

Limiting the opening of files and folders to a limited set reduces the attack surface of the system.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer:PreXPSP2ShellProtocolBehavior
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\File Explorer\Turn off shell protocol protected mode
```

Note: This Group Policy path is provided by the Group Policy template **WindowsExplorer.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (The protocol is in the protected mode, allowing applications to only open a limited set of folders.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224943
Rule ID: SV-224943r569186_rule
STIG ID: WN16-CC-000360
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	8.3 <u>Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies</u> Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.			

18.10.29 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).

18.10.30 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).

18.10.31 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).

18.10.32 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).

18.10.33 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).

18.10.34 Internet Explorer

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template **InetRes.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

CIS publishes security guidance for Microsoft Internet Explorer in a separate benchmark from Windows. Additional details can be found in the [CIS Microsoft Web Browser Benchmarks Community](#).

18.10.35 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.

18.10.36 Location and Sensors

This section contains settings for Locations and Sensors.

This Group Policy section is provided by the Group Policy template **Sensors.admx/adml** that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.10.36.1 Ensure 'Turn off location' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting turns off the location feature for the computer.

The recommended state for this setting is: **Enabled**.

Rationale:

This setting affects the location feature (e.g. GPS or other location tracking). From a security perspective, it's not a good idea to reveal your location to software in most cases, but there are legitimate uses, such as mapping software. However, they should not be used in high security environments.

Impact:

The location feature is turned off, and all programs on the computer are prevented from using location information from the location feature.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\LocationAndSensors:DisableLocation
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Location and Sensors\Turn off location
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **Sensors.admx/adml** that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

Disabled. (Programs on the computer are permitted to use location information from the location feature.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

18.10.37 Maintenance Scheduler

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `msched.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.10.38 Maps

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WinMaps.admx/adml` that is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).

18.10.39 MDM

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `MDM.admx/adml` that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

18.10.40 Messaging

This section contains messaging settings.

This Group Policy section is provided by the Group Policy template `Messaging.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

18.10.40.1 Ensure 'Allow Message Service Cloud Sync' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting allows backup and restore of cellular text messages to Microsoft's cloud services.

The recommended state for this setting is: **Disabled**.

Rationale:

In a high security environment, data should never be sent to any third-party since this data could contain sensitive information.

Impact:

Cellular text messages will not be backed up to (or restored from) Microsoft's cloud services.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Messaging:AllowMessageSync
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Messaging\Allow Message Service Cloud Sync
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **Messaging.admx/adml** that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Default Value:

Enabled. (Cellular text messages can be backed up and restored to Microsoft's cloud services.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

18.10.41 Microsoft account

This section contains recommendations related to Microsoft Accounts.

This Group Policy section is provided by the Group Policy template [MSAPolicy.admx/adml](#) that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

18.10.41.1 Ensure 'Block all consumer Microsoft account user authentication' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This setting determines whether applications and services on the device can utilize new consumer Microsoft account authentication via the Windows **OnlineID** and **WebAccountManager** APIs.

The recommended state for this setting is: **Enabled**.

Rationale:

Organizations that want to effectively implement identity management policies and maintain firm control of what accounts are used on their computers will probably want to block Microsoft accounts. Organizations may also need to block Microsoft accounts in order to meet the requirements of compliance standards that apply to their information systems.

Impact:

All applications and services on the device will be prevented from *new* authentications using consumer Microsoft accounts via the Windows **OnlineID** and **WebAccountManager** APIs. Authentications performed directly by the user in web browsers or in apps that use **OAuth** will remain unaffected.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

HKLM\SOFTWARE\Policies\Microsoft\MicrosoftAccount:DisableUserAuth

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Microsoft accounts\Block all consumer Microsoft account user  
authentication
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **MSAPolicy.admx/adml** that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

Default Value:

Disabled. (Applications and services on the device will be permitted to authenticate using consumer Microsoft accounts via the Windows **OnlineID** and **WebAccountManager** APIs.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.6 Centralize Account Management Centralize account management through a directory or identity service.			
v7	16.8 Disable Any Unassociated Accounts Disable any account that cannot be associated with a business process or business owner.			

18.10.42 Microsoft Defender Antivirus (formerly Windows Defender and Windows Defender Antivirus)

This section 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 Windows 10 Release 2004 Administrative Templates.

18.10.42.1 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).

18.10.42.2 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).

18.10.42.3 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).

18.10.42.4 Features

This section is 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 22H2 Administrative Templates v1.0 (or newer).

18.10.42.5 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).

18.10.42.5.1 Ensure 'Configure local setting override for reporting to Microsoft MAPS' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting configures a local override for the configuration to join Microsoft Active Protection Service (MAPS), which Microsoft has now renamed to "Microsoft Defender Antivirus Cloud Protection Service". This setting can only be set by Group Policy.

The recommended state for this setting is: **Disabled**.

Rationale:

The decision on whether or not to participate in Microsoft MAPS / Microsoft Defender Antivirus Cloud Protection Service for malicious software reporting should be made centrally in an enterprise managed environment, so that all computers within it behave consistently in that regard. Configuring this setting to Disabled ensures that the decision remains centrally managed.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows  
Defender\Spynet:LocalSettingOverrideSpynetReporting
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Microsoft Defender Antivirus\MAPS\Configure local setting override  
for reporting to Microsoft MAPS
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **WindowsDefender.admx/adml** that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Disabled. (Group Policy will take priority over the local preference setting.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

18.10.42.5.2 Ensure 'Join Microsoft MAPS' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting allows you to join Microsoft Active Protection Service (MAPS), which Microsoft has now renamed to *Windows Defender Antivirus Cloud Protection Service* and then *Microsoft Defender Antivirus Cloud Protection Service*. Microsoft MAPS / Microsoft Defender Antivirus Cloud Protection Service is the online community that helps you choose how to respond to potential threats. The community also helps stop the spread of new malicious software infections. You can choose to send basic or additional information about detected software. Additional information helps Microsoft create new definitions and help it to protect your computer.

Possible options are:

- (0x0) Disabled (default)
- (0x1) Basic membership
- (0x2) Advanced membership

Basic membership will send basic information to Microsoft about software that has been detected including where the software came from the actions that you apply or that are applied automatically and whether the actions were successful.

Advanced membership in addition to basic information will send more information to Microsoft about malicious software spyware and potentially unwanted software including the location of the software file names how the software operates and how it has impacted your computer.

The recommended state for this setting is: **Disabled**.

Note: In Windows 10 and above, Basic membership is no longer available, so setting the value to **1** Basic, or **2** Advanced, enrolls the device into Advanced membership. For more information, please visit: [Turn on cloud protection in Microsoft Defender Antivirus - Microsoft Defender for Endpoint | Microsoft Learn](#).

Rationale:

The information that would be sent can include things like location of detected items on your computer if harmful software was removed. The information would be automatically collected and sent. In some instances personal information might unintentionally be sent to Microsoft. However, Microsoft states that it will not use this information to identify you or contact you.

For privacy reasons in high security environments, it is best to prevent these data submissions altogether.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0** or that the key **does not exist**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet:SpynetReporting
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Microsoft Defender Antivirus\MAPS\Join Microsoft MAPS
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **WindowsDefender.admx/adml** that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Disabled. (Microsoft MAPS / Microsoft Defender Antivirus Cloud Protection Service will not be joined.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

18.10.42.6 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.

18.10.42.6.1 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).

18.10.42.6.1.1 Ensure 'Configure Attack Surface Reduction rules' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls the state for the Attack Surface Reduction (ASR) rules.

The recommended state for this setting is: **Enabled**.

Rationale:

Attack surface reduction helps prevent actions and apps that are typically used by exploit-seeking malware to infect machines.

Impact:

When a rule is triggered, a notification will be displayed from the Action Center.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR:ExploitGuard_ASR_Rules
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Microsoft Defender Exploit Guard\Attack Surface Reduction\Configure Attack Surface Reduction rules
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **WindowsDefender.admx/adml** that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Default Value:

Disabled. (No ASR rules will be configured.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 <u>Enable Anti-Exploitation Features</u> Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 <u>Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies</u> Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

18.10.42.6.1.2 Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is configured (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting sets the Attack Surface Reduction rules.

The recommended state for this setting is:

26190899-1602-49e8-8b27-eb1d0a1ce869 - 1 (Block Office communication application from creating child processes)
3b576869-a4ec-4529-8536-b80a7769e899 - 1 (Block Office applications from creating executable content)
56a863a9-875e-4185-98a7-b882c64b5ce5 - 1 (Block abuse of exploited vulnerable signed drivers)
5beb7efe-fd9a-4556-801d-275e5ffc04cc - 1 (Block execution of potentially obfuscated scripts)
75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84 - 1 (Block Office applications from injecting code into other processes)
7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c - 1 (Block Adobe Reader from creating child processes)
9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2 - 1 (Block credential stealing from the Windows local security authority subsystem (lsass.exe))
b2b3f03d-6a65-4f7b-a9c7-1c7ef74a9ba4 - 1 (Block untrusted and unsigned processes that run from USB)
be9ba2d9-53ea-4cdc-84e5-9b1eeee46550 - 1 (Block executable content from email client and webmail)
d4f940ab-401b-4efc-aadc-ad5f3c50688a - 1 (Block Office applications from creating child processes)

Note: More information on ASR rules can be found at the following link: [Use Attack surface reduction rules to prevent malware infection | Microsoft Docs](#)

Rationale:

Attack surface reduction helps prevent actions and apps that are typically used by exploit-seeking malware to infect machines.

Impact:

When a rule is triggered, a notification will be displayed from the Action Center.

Note: The following rules apply to Windows Server 2019 and 2022, but do not apply to Windows Server 2012 R2 and 2016: **92e97fa1-2edf-4476-bdd6-9dd0b4dddc7b** (Block Win32 API calls from Office macro), **d3e037e1-3eb8-44c8-a917-57927947596d** (Block JavaScript or VBScript from launching downloaded executable content), and **e6db77e5-3df2-4cf1-b95a-636979351e5b** (Block persistence through WMI event subscription).

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry locations with a **REG_SZ** value of **1**.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:26190899-1602-49e8-8b27-eb1d0a1ce869
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:3b576869-a4ec-4529-8536-b80a7769e899
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:56a863a9-875e-4185-98a7-b882c64b5ce5
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:5beb7efe-fd9a-4556-801d-275e5ffc04cc
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:9e6c4e1f-7d60-472f-bala-a39ef669e4b2
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:b2b3f03d-6a65-4f7b-a9c7-1c7ef74a9ba4
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:be9ba2d9-53ea-4cdc-84e5-9bleeee46550
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:d4f940ab-401b-4efc-aadc-ad5f3c50688a
```


Remediation:

To establish the recommended configuration via GP, set the following UI path so that 26190899-1602-49e8-8b27-eb1d0a1ce869, 3b576869-a4ec-4529-8536-b80a7769e899, 56a863a9-875e-4185-98a7-b882c64b5ce5, 5beb7efe-fd9a-4556-801d-275e5ffc04cc, 75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84, 7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c, 9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2, b2b3f03d-6a65-4f7b-a9c7-1c7ef74a9ba4, be9ba2d9-53ea-4cdc-84e5-9b1eeee46550, and d4f940ab-401b-4efc-aadc-ad5f3c50688a are each set to a value of 1:

Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Microsoft Defender Exploit Guard\Attack Surface Reduction\Configure Attack Surface Reduction rules: Set the state for each ASR rule

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template [WindowsDefender.admx/adml](#) that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Default Value:

Disabled. (No ASR rules will be configured.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

18.10.42.6.2 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).

18.10.42.6.3 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).

18.10.42.6.3.1 Ensure 'Prevent users and apps from accessing dangerous websites' is set to 'Enabled: Block' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls Microsoft Defender Exploit Guard network protection.

The recommended state for this setting is: **Enabled: Block**.

Rationale:

This setting can help prevent employees from using any application to access dangerous domains that may host phishing scams, exploit-hosting sites, and other malicious content on the Internet.

Impact:

Users and applications will not be able to access dangerous domains.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\Network Protection\EnableNetworkProtection
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled: Block**:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Microsoft Defender Exploit Guard\Network Protection\Prevent users and apps from accessing dangerous websites
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **WindowsDefender.admx/adml** that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Default Value:

Disabled. (Users and applications will not be blocked from connecting to dangerous domains.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.3 <u>Maintain and Enforce Network-Based URL Filters</u> Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.			
v8	10.5 <u>Enable Anti-Exploitation Features</u> Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.			
v7	7.4 <u>Maintain and Enforce Network-Based URL Filters</u> Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.			
v7	8.3 <u>Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies</u> Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.			

18.10.42.7 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).

18.10.42.7.1 Ensure 'Enable file hash computation feature' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This setting determines whether hash values are computed for files scanned by Microsoft Defender.

The recommended state for this setting is: **Enabled**.

Rationale:

When running an antivirus solution such as Microsoft Defender Antivirus, it is important to ensure that it is configured to monitor for suspicious and known malicious activity. File hashes are a reliable way of detecting changes to files, and can speed up the scan process by skipping files that have not changed since they were last scanned and determined to be safe. A changed file hash can also be cause for additional scrutiny.

Impact:

This setting could cause performance degradation during initial deployment and for users where new executable content is frequently being created (such as software developers), or where applications are frequently installed or updated.

For more information on this setting, please visit [Security baseline \(FINAL\): Windows 10 and Windows Server, version 2004 - Microsoft Tech Community - 1543631](#).

Note: The impact of this setting should be monitored closely during deployment to ensure user and system performance impact is within acceptable limits.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows  
Defender\MpEngine:EnableFileHashComputation
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Microsoft Defender Antivirus\MpEngine\Enable file hash computation  
feature
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **WindowsDefender.admx/adml** that is included with the Microsoft Windows 10 Release 2004 Administrative Templates (or newer).

Default Value:

Disabled. (File hash values are not computed during scans.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 <u>Deploy and Maintain Anti-Malware Software</u> Deploy and maintain anti-malware software on all enterprise assets.			
v7	8.1 <u>Utilize Centrally Managed Anti-malware Software</u> Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.			

18.10.42.8 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).

18.10.42.9 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).

18.10.42.10 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).

18.10.42.10.1 Ensure 'Scan all downloaded files and attachments' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting configures scanning for all downloaded files and attachments.

The recommended state for this setting is: **Enabled**.

Rationale:

When running an antivirus solution such as Microsoft Defender Antivirus, it is important to ensure that it is configured to heuristically monitor in real-time for suspicious and known malicious activity.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time  
Protection:DisableIOAVProtection
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Microsoft Defender Antivirus\Real-Time Protection\Scan all  
downloaded files and attachments
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **WindowsDefender.admx/adml** that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Enabled. (All downloaded files and attachments will be scanned.)

References:

1. <https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-antivirus/configure-real-time-protection-microsoft-defender-antivirus>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 <u>Deploy and Maintain Anti-Malware Software</u> Deploy and maintain anti-malware software on all enterprise assets.			
v7	8.1 <u>Utilize Centrally Managed Anti-malware Software</u> Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.			

18.10.42.10.2 Ensure 'Turn off real-time protection' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting configures real-time protection prompts for known malware detection.

Microsoft Defender Antivirus alerts you when malware or potentially unwanted software attempts to install itself or to run on your computer.

The recommended state for this setting is: **Disabled**.

Rationale:

When running an antivirus solution such as Microsoft Defender Antivirus, it is important to ensure that it is configured to heuristically monitor in real-time for suspicious and known malicious activity.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time  
Protection:DisableRealtimeMonitoring
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Microsoft Defender Antivirus\Real-Time Protection\Turn off real-  
time protection
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **WindowsDefender.admx/adml** that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Disabled. (Microsoft Defender Antivirus will prompt users to take actions on malware detections.)

References:

1. <https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-antivirus/configure-real-time-protection-microsoft-defender-antivirus>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 <u>Deploy and Maintain Anti-Malware Software</u> Deploy and maintain anti-malware software on all enterprise assets.			
v7	8.1 <u>Utilize Centrally Managed Anti-malware Software</u> Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.			

18.10.42.10.3 Ensure 'Turn on behavior monitoring' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to configure behavior monitoring for Microsoft Defender Antivirus.

The recommended state for this setting is: **Enabled**.

Rationale:

When running an antivirus solution such as Microsoft Defender Antivirus, it is important to ensure that it is configured to heuristically monitor in real-time for suspicious and known malicious activity.

Impact:

None - this is the default configuration.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time  
Protection:DisableBehaviorMonitoring
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Microsoft Defender Antivirus\Real-Time Protection\Turn on behavior  
monitoring
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **WindowsDefender.admx/adml** that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Enabled. (Behavior monitoring will be enabled.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.7 <u>Use Behavior-Based Anti-Malware Software</u> Use behavior-based anti-malware software.		●	●
v7	8.1 <u>Utilize Centrally Managed Anti-malware Software</u> Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

18.10.42.10.4 Ensure 'Turn on script scanning' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows script scanning to be turned on/off. Script scanning intercepts scripts then scans them before they are executed on the system.

The recommended state for this setting is: **Enabled**.

Rationale:

When running an antivirus solution such as Microsoft Defender Antivirus, it is important to ensure that it is configured to heuristically monitor in real-time for suspicious and known malicious activity.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time  
Protection:DisableScriptScanning
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Microsoft Defender Antivirus\Real-Time Protection\Turn on script  
scanning
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **WindowsDefender.admx/adml** that is included with the Microsoft Windows 11 Release 21H2 Administrative Templates (or newer).

Default Value:

Enabled. (Script scanning will be enabled.)

References:

1. <https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-advanced-scan-types-microsoft-defender-antivirus?view=o365-worldwide>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.7 <u>Use Behavior-Based Anti-Malware Software</u> Use behavior-based anti-malware software.			
v7	8.1 <u>Utilize Centrally Managed Anti-malware Software</u> Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.			

18.10.42.11 Remediation

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template [WindowsDefender.admx/adml](#) that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.10.42.12 Reporting

This section contains settings related to Microsoft Defender Antivirus 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).

18.10.42.12.1 Ensure 'Configure Watson events' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting allows you to configure whether or not Watson events are sent.

The recommended state for this setting is: **Disabled**.

Rationale:

Watson events are the reports that get sent to Microsoft when a program or service crashes or fails, including the possibility of automatic submission. Preventing this information from being sent can help reduce privacy concerns.

Impact:

Watson events will not be sent to Microsoft automatically when a program or service crashes or fails.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows  
Defender\Reporting\DisableGenericRePorts
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Microsoft Defender Antivirus\Reporting\Configure Watson events
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **WindowsDefender.admx/adml** that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Enabled. (Watson events *will* be sent to Microsoft automatically when a program or service crashes or fails.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	13.3 <u>Monitor and Block Unauthorized Network Traffic</u> Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.			●

18.10.42.13 Scan

This section contains settings related to Microsoft Defender Antivirus 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).

18.10.42.13.1 Ensure 'Scan packed executables' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting manages whether or not Microsoft Defender Antivirus scans packed executables. Packed executables are executable files that contain compressed code.

The recommended state for this setting is: **Enabled**.

Rationale:

Packing executables is a way to compress and create smaller files and can make it difficult to access and analyze the code associated with the executable. This is a common method to obfuscate malicious executables by bad actors.

Impact:

None - This is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows  
Defender\Scan:DisablePackedExeScanning
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Microsoft Defender Antivirus\Scan\Scan packed executables
```

Note: This Group Policy path is provided by the Group Policy template **WindowsDefender.admx/adml** that is included with the Microsoft Windows 8.1 and Server 2012 R2 Administrative Templates (or newer).

Default Value:

Enabled. (Packed executables will be scanned.)

References:

1. <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-advanced-scan-types-microsoft-defender-antivirus?view=o365-worldwide#settings-and-locations>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>10.4 Configure Automatic Anti-Malware Scanning of Removable Media</u> Configure anti-malware software to automatically scan removable media.			
v7	<u>8.4 Configure Anti-Malware Scanning of Removable Devices</u> Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.			

18.10.42.13.2 Ensure 'Scan removable drives' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting manages whether or not to scan for malicious software and unwanted software in the contents of removable drives, such as USB flash drives, when running a full scan.

The recommended state for this setting is: **Enabled**.

Rationale:

It is important to ensure that any present removable drives are always included in any type of scan, as removable drives are more likely to contain malicious software brought in to the enterprise managed environment from an external, unmanaged computer.

Impact:

Removable drives will be scanned during any type of scan by Microsoft Defender Antivirus.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows  
Defender\Scan:DisableRemovableDriveScanning
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Microsoft Defender Antivirus\Scan\Scan removable drives
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **WindowsDefender.admx/adml** that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Disabled. (Removable drives will not be scanned during a full scan. Removable drives may still be scanned during quick scan and custom scan.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>10.4 Configure Automatic Anti-Malware Scanning of Removable Media</u> Configure anti-malware software to automatically scan removable media.			
v7	<u>8.4 Configure Anti-Malware Scanning of Removable Devices</u> Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.			

18.10.42.13.3 Ensure 'Turn on e-mail scanning' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

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.

Impact:

E-mail scanning by Microsoft Defender Antivirus will be enabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Scan:DisableEmailScanning
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Scan\Turn on e-mail scanning
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **WindowsDefender.admx/adml** that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Disabled. (E-mail scanning by Microsoft Defender Antivirus will be disabled.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 <u>Deploy and Maintain Anti-Malware Software</u> Deploy and maintain anti-malware software on all enterprise assets.			
v7	8.1 <u>Utilize Centrally Managed Anti-malware Software</u> Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.			

18.10.42.14 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.

18.10.42.15 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).

18.10.42.16 Ensure 'Configure detection for potentially unwanted applications' is set to 'Enabled: Block' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls detection and action for Potentially Unwanted Applications (PUA), which are sneaky unwanted application bundlers or their bundled applications, that can deliver adware or malware.

The recommended state for this setting is: **Enabled: Block**.

For more information, see this link: [Block potentially unwanted applications with Microsoft Defender Antivirus | Microsoft Docs](#)

Rationale:

Potentially unwanted applications can increase the risk of your network being infected with malware, cause malware infections to be harder to identify, and can waste IT resources in cleaning up the applications. They should be blocked from installation.

Impact:

Applications that are identified by Microsoft as PUA will be blocked at download and install time.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

This group policy setting is backed by the following registry location with a REG_DWORD value of 1.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender:PUAProtection
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled: Block**:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Configure detection for potentially unwanted applications
```

Note: This Group Policy path is provided by the Group Policy template **WindowsDefender.admx/adml** that is included with the Microsoft Windows 10 Release 1809 & Server 2019 Administrative Templates (or newer).

Default Value:

Disabled. (Applications that are identified by Microsoft as PUA will not be blocked.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 <u>Deploy and Maintain Anti-Malware Software</u> Deploy and maintain anti-malware software on all enterprise assets.			
v7	2.7 <u>Utilize Application Whitelisting</u> Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.			
v7	8.1 <u>Utilize Centrally Managed Anti-malware Software</u> Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.			

18.10.42.17 Ensure 'Turn off Microsoft Defender AntiVirus' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting turns off Microsoft Defender Antivirus. If the setting is configured to Disabled, Microsoft Defender Antivirus runs and computers are scanned for malware and other potentially unwanted software.

The recommended state for this setting is: **Disabled**.

Rationale:

It is important to ensure a current, updated antivirus product is scanning each computer for malicious file activity. Microsoft provides a competent solution out of the box in Microsoft Defender Antivirus.

Organizations that choose to purchase a reputable third-party antivirus solution may choose to exempt themselves from this recommendation in lieu of the commercial alternative.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

HKLM\SOFTWARE\Policies\Microsoft\Windows Defender:DisableAntiSpyware

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Turn off Microsoft Defender AntiVirus

Note: This Group Policy path is provided by the Group Policy template **WindowsDefender.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Turn off Windows Defender*, but it was renamed starting with the Windows 10 Release 1703 Administrative Templates. It was again renamed to *Windows Defender Antivirus* starting with the Windows 10 Release 2004 Administrative Templates.

Default Value:

Disabled. (Microsoft Defender Antivirus runs and computers are scanned for malware and other potentially unwanted software.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 <u>Deploy and Maintain Anti-Malware Software</u> Deploy and maintain anti-malware software on all enterprise assets.			
v7	8.1 <u>Utilize Centrally Managed Anti-malware Software</u> Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.			

18.10.43 Microsoft Defender Application Guard (formerly Windows Defender Application Guard)

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template [AppHVSI.admx/adml](#) that is included with the Microsoft Windows 10 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.

18.10.44 Microsoft Defender Exploit Guard (formerly Windows Defender Exploit Guard)

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template [ExploitGuard.admx/adml](#) that is included with the Microsoft Windows 10 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.

18.10.45 Microsoft Edge

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template [MicrosoftEdge.admx/adml](#) that is included with the Microsoft Windows 10 RTM (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](#).

18.10.46 Microsoft Secondary Authentication Factor

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template [DeviceCredential.admx/adml](#) that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

18.10.47 Microsoft User Experience Virtualization

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template [UserExperienceVirtualization.admx/adml](#) that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

18.10.48 NetMeeting

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template [Conf.admx/adml](#) that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.49 News and interests

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template [Feeds.admx/adml](#) that is included with the Microsoft Windows 10 Release 21H1 Administrative Templates (or newer).

18.10.50 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.

18.10.50.1 Ensure 'Prevent the usage of OneDrive for file storage' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting lets you prevent apps and features from working with files on OneDrive using the Next Generation Sync Client.

The recommended state for this setting is: **Enabled**.

Rationale:

Enabling this setting prevents users from accidentally (or intentionally) uploading confidential or sensitive corporate information to the OneDrive cloud service using the Next Generation Sync Client.

Note: This security concern applies to *any* cloud-based file storage application installed on a server, not just the one supplied with Windows Server.

Impact:

Users can't access OneDrive from the OneDrive app and file picker. Windows Store apps can't access OneDrive using the WinRT API. OneDrive doesn't appear in the navigation pane in File Explorer. OneDrive files aren't kept in sync with the cloud. Users can't automatically upload photos and videos from the camera roll folder.

Note: If your organization uses Office 365, be aware that this setting will prevent users from saving files to OneDrive/SkyDrive.

Note #2: If your organization has decided to implement **OneDrive for Business** and therefore needs to except itself from this recommendation, we highly suggest that you also obtain and utilize the **OneDrive.admx/adml** template that is bundled with the latest OneDrive client, as noted [at this link](#) (this template is not included with the Windows Administrative Templates). Two alternative OneDrive settings in particular from that template are worth your consideration:

- *Allow syncing OneDrive accounts for only specific organizations* - a computer-based setting that restricts OneDrive client connections to only **approved** tenant IDs.
- *Prevent users from synchronizing personal OneDrive accounts* - a user-based setting that prevents use of consumer OneDrive (i.e. non-business).

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\OneDrive:DisableFileSyncNGSC
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\OneDrive\Prevent the usage of OneDrive for file storage
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **SkyDrive.admx/adml** that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer). However, we strongly recommend you only use the version included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer). Older versions of the templates had conflicting settings in different template files for both OneDrive & SkyDrive, until it was cleaned up properly in the above version.

Note #2: In older Microsoft Windows Administrative Templates, this setting was named *Prevent the usage of SkyDrive for file storage*, but it was renamed starting with the Windows 10 RTM (Release 1507) Administrative Templates.

Default Value:

Disabled. (Apps and features can work with OneDrive file storage using the Next Generation Sync Client.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>13.4 Only Allow Access to Authorized Cloud Storage or Email Providers</u> Only allow access to authorized cloud storage or email providers.			

18.10.51 Online Assistance

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template [HelpAndSupport.admx/adml](#) that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.52 OOB

This section is 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).

18.10.53 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).

18.10.54 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.

18.10.55 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).

18.10.55.1 Ensure 'Turn off Push To Install service' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting controls whether users can push Apps to the device from the Microsoft Store App running on other devices or the web.

The recommended state for this setting is: **Enabled**.

Rationale:

In a high security managed environment, application installations should be managed centrally by IT staff, not by end users.

Impact:

Users will not be able to push Apps to this device from the Microsoft Store running on other devices or the web.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\PushToInstall:DisablePushToInstall
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Push to Install\Turn off Push To Install service
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **PushToInstall.admx/adml** that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Default Value:

Disabled. (Users are able to push Apps to this device from the Microsoft Store running on other devices or the web.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.5 <u>Allowlist Authorized Software</u> Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.			
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

18.10.56 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.

18.10.56.1 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.

18.10.56.2 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.

18.10.56.2.1 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).

18.10.56.2.2 Ensure 'Do not allow passwords to be saved' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting helps prevent Remote Desktop clients from saving passwords on a computer.

The recommended state for this setting is: **Enabled**.

Note: If this policy setting was previously configured as Disabled or Not configured, any previously saved passwords will be deleted the first time a Remote Desktop client disconnects from any server.

Rationale:

An attacker with physical access to the computer may be able to break the protection guarding saved passwords. An attacker who compromises a user's account and connects to their computer could use saved passwords to gain access to additional hosts.

Impact:

The password saving checkbox will be disabled for Remote Desktop clients and users will not be able to save passwords.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal  
Services:DisablePasswordSaving
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Remote Desktop Services\Remote Desktop Connection Client\Do not
allow passwords to be saved
```

Note: This Group Policy path is provided by the Group Policy template **TerminalServer.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Users will be able to save passwords using Remote Desktop Connection.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224944
Rule ID: SV-224944r852332_rule
STIG ID: WN16-CC-000370
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	16.11 <u>Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity.			

18.10.56.3 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.

18.10.56.3.1 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).

18.10.56.3.2 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.

18.10.56.3.2.1 Ensure 'Restrict Remote Desktop Services users to a single Remote Desktop Services session' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting allows you to restrict users to a single Remote Desktop Services session.

The recommended state for this setting is: **Enabled**.

Rationale:

This setting ensures that users & administrators who Remote Desktop to a server will continue to use the same session - if they disconnect and reconnect, they will go back to the same session they were using before, preventing the creation of a second simultaneous session. This both prevents unnecessary resource usage by having the server host unnecessary additional sessions (which would put extra load on the server) and also ensures a consistency of experience for the user.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal  
Services:fSingleSessionPerUser
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Remote Desktop Services\Remote Desktop Session  
Host\Connections\Restrict Remote Desktop Services users to a single Remote  
Desktop Services session
```

Note: This Group Policy path is provided by the Group Policy template **TerminalServer.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was named *Restrict Terminal Services users to a single remote session*, but it was renamed starting with the Windows 7 & Server 2008 R2 Administrative Templates.

Default Value:

Enabled. (Users who log on remotely by using Remote Desktop Services will be restricted to a single session (either active or disconnected) on that server. If the user leaves the session in a disconnected state, the user automatically reconnects to that session at the next logon.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

18.10.56.3.3 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.

18.10.56.3.3.1 Ensure 'Do not allow COM port redirection' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting specifies whether to prevent the redirection of data to client COM ports from the remote computer in a Remote Desktop Services session.

The recommended state for this setting is: **Enabled**.

Rationale:

In a more security-sensitive environment, it is desirable to reduce the possible attack surface. The need for COM port redirection within a Remote Desktop session is very rare, so makes sense to reduce the number of unexpected avenues for data exfiltration and/or malicious code transfer.

Impact:

Users in a Remote Desktop Services session will not be able to redirect server data to local (client) COM ports.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:fDisableCcm
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection\Do not allow COM port redirection
```

Note: This Group Policy path is provided by the Group Policy template **TerminalServer.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Remote Desktop Services allows COM port redirection.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

18.10.56.3.3.2 Ensure 'Do not allow drive redirection' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting prevents users from sharing the local drives on their client computers to Remote Desktop Servers that they access. Mapped drives appear in the session folder tree in Windows Explorer in the following format:

`\\TSClient\<driveletter>$`

If local drives are shared they are left vulnerable to intruders who want to exploit the data that is stored on them.

The recommended state for this setting is: **Enabled**.

Rationale:

Data could be forwarded from the user's Remote Desktop Services session to the user's local computer without any direct user interaction. Malicious software already present on a compromised server would have direct and stealthy disk access to the user's local computer during the Remote Desktop session.

Impact:

Drive redirection will not be possible. In most situations, traditional network drive mapping to file shares (including administrative shares) performed manually by the connected user will serve as a capable substitute to still allow file transfers when needed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:fDisableCdm

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection\Do not allow drive redirection

Note: This Group Policy path is provided by the Group Policy template **TerminalServer.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (An RD Session Host maps client drives automatically upon connection.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224945
Rule ID: SV-224945r569186_rule
STIG ID: WN16-CC-000380
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

18.10.56.3.3.3 Ensure 'Do not allow LPT port redirection' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting specifies whether to prevent the redirection of data to client LPT ports during a Remote Desktop Services session.

The recommended state for this setting is: **Enabled**.

Rationale:

In a more security-sensitive environment, it is desirable to reduce the possible attack surface. The need for LPT port redirection within a Remote Desktop session is very rare, so makes sense to reduce the number of unexpected avenues for data exfiltration and/or malicious code transfer.

Impact:

Users in a Remote Desktop Services session will not be able to redirect server data to local (client) LPT ports.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:fDisableLPT
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection\Do not allow LPT port redirection
```

Note: This Group Policy path is provided by the Group Policy template **TerminalServer.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Remote Desktop Services allows LPT port redirection.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

18.10.56.3.3.4 Ensure 'Do not allow supported Plug and Play device redirection' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting allows you to control the redirection of supported Plug and Play devices, such as Windows Portable Devices, to the remote computer in a Remote Desktop Services session.

The recommended state for this setting is: **Enabled**.

Rationale:

In a more security-sensitive environment, it is desirable to reduce the possible attack surface. The need for Plug and Play device redirection within a Remote Desktop session is very rare, so makes sense to reduce the number of unexpected avenues for data exfiltration and/or malicious code transfer.

Impact:

Users in a Remote Desktop Services session will not be able to redirect their supported (local client) Plug and Play devices to the remote computer.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal  
Services:fDisablePNPRedir
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Remote Desktop Services\Remote Desktop Session Host\Device and  
Resource Redirection\Do not allow supported Plug and Play device redirection
```

Note: This Group Policy path is provided by the Group Policy template **TerminalServer.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Remote Desktop Services allows redirection of supported Plug and Play devices.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

18.10.56.3.4 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.

18.10.56.3.5 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.

18.10.56.3.6 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.

18.10.56.3.7 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.

18.10.56.3.8 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.

18.10.56.3.9 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.

18.10.56.3.9.1 Ensure 'Always prompt for password upon connection' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting specifies whether Remote Desktop Services always prompts the client computer for a password upon connection. You can use this policy setting to enforce a password prompt for users who log on to Remote Desktop Services, even if they already provided the password in the Remote Desktop Connection client.

The recommended state for this setting is: **Enabled**.

Rationale:

Users have the option to store both their username and password when they create a new Remote Desktop Connection shortcut. If the server that runs Remote Desktop Services allows users who have used this feature to log on to the server but not enter their password, then it is possible that an attacker who has gained physical access to the user's computer could connect to a Remote Desktop Server through the Remote Desktop Connection shortcut, even though they may not know the user's password.

Impact:

Users cannot automatically log on to Remote Desktop Services by supplying their passwords in the Remote Desktop Connection client. They will be prompted for a password to log on.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal  
Services:fPromptForPassword
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Remote Desktop Services\Remote Desktop Session  
Host\Security\Always prompt for password upon connection
```

Note: This Group Policy path is provided by the Group Policy template **TerminalServer.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In the Microsoft Windows Vista Administrative Templates, this setting was named *Always prompt client for password upon connection*, but it was renamed starting with the Windows Server 2008 (non-R2) Administrative Templates.

Default Value:

Disabled. (Remote Desktop Services allows users to automatically log on if they enter a password in the Remote Desktop Connection client.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224946
Rule ID: SV-224946r852333_rule
STIG ID: WN16-CC-000390
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

18.10.56.3.9.2 Ensure 'Require secure RPC communication' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting allows you to specify whether Remote Desktop Services requires secure Remote Procedure Call (RPC) communication with all clients or allows unsecured communication.

You can use this policy setting to strengthen the security of RPC communication with clients by allowing only authenticated and encrypted requests.

The recommended state for this setting is: **Enabled**.

Rationale:

Allowing unsecure RPC communication can exposes the server to man in the middle attacks and data disclosure attacks.

Impact:

Remote Desktop Services accepts requests from RPC clients that support secure requests, and does not allow unsecured communication with untrusted clients.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal  
Services:fEncryptRPCTraffic
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Remote Desktop Services\Remote Desktop Session
Host\Security\Require secure RPC communication
```

Note: This Group Policy path is provided by the Group Policy template **TerminalServer.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Remote Desktop Services always requests security for all RPC traffic. However, unsecured communication is allowed for RPC clients that do not respond to the request.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224947
Rule ID: SV-224947r877394_rule
STIG ID: WN16-CC-000400
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.10 <u>Perform Application Layer Filtering</u> Perform application layer filtering. Example implementations include a filtering proxy, application layer firewall, or gateway.			

18.10.56.3.9.3 Ensure 'Require use of specific security layer for remote (RDP) connections' is set to 'Enabled: SSL' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting specifies whether to require the use of a specific security layer to secure communications between clients and RD Session Host servers during Remote Desktop Protocol (RDP) connections.

The recommended state for this setting is: **Enabled: SSL**.

Note: In spite of this setting being labeled *SSL*, it is actually enforcing Transport Layer Security (TLS) version 1.0, not the older (and less secure) SSL protocol.

Rationale:

The native Remote Desktop Protocol (RDP) encryption is now considered a weak protocol, so enforcing the use of stronger Transport Layer Security (TLS) encryption for all RDP communications between clients and RD Session Host servers is preferred.

Impact:

TLS 1.0 will be required to authenticate to the RD Session Host server. If TLS is not supported, the connection fails.

Note: By default, this setting will use a self-signed certificate for RDP connections. If your organization has established the use of a Public Key Infrastructure (PKI) for SSL/TLS encryption, then we recommend that you also configure the *Server authentication certificate template* setting to instruct RDP to use a certificate from your PKI instead of a self-signed one. Note that the certificate template used for this purpose must have “Client Authentication” configured as an Intended Purpose. Note also that a valid, non-expired certificate using the specified template must already be installed on the server for it to work.

Note #2: Some third party two-factor authentication solutions (e.g. RSA Authentication Agent) can be negatively affected by this setting, as the SSL/TLS security layer will expect the user's Windows password upon initial connection attempt (before the RDP logon screen), and once successfully authenticated, pass the credential along to that Windows session on the RDP host (to complete the login). If a two-factor agent is present and expecting a different credential at the RDP logon screen, this initial connection may result in a failed logon attempt, and also effectively cause a “double logon” requirement for each and every new RDP session.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **2**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services\SecurityLayer
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled: SSL**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Remote Desktop Services\Remote Desktop Session  
Host\Security\Require use of specific security layer for remote (RDP)  
connections
```

Note: This Group Policy path is provided by the Group Policy template **TerminalServer.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Negotiate. (The most secure method that is supported by the client is enforced. If TLS is supported, it is used to authenticate the RD Session Host server. If TLS is not supported, native RDP encryption is used, but the RD Session Host server is not authenticated.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			

18.10.56.3.9.4 Ensure 'Require user authentication for remote connections by using Network Level Authentication' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to specify whether to require user authentication for remote connections to the RD Session Host server by using Network Level Authentication.

The recommended state for this setting is: **Enabled**.

Rationale:

Requiring that user authentication occur earlier in the remote connection process enhances security.

Impact:

Only client computers that support Network Level Authentication can connect to the RD Session Host server.

Note: Some third party two-factor authentication solutions (e.g. RSA Authentication Agent) can be negatively affected by this setting, as Network Level Authentication will expect the user's Windows password upon initial connection attempt (before the RDP logon screen), and once successfully authenticated, pass the credential along to that Windows session on the RDP host (to complete the login). If a two-factor agent is present and expecting a different credential at the RDP logon screen, this initial connection may result in a failed logon attempt, and also effectively cause a “double logon” requirement for each and every new RDP session.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal  
Services\UserAuthentication
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Remote Desktop Services\Remote Desktop Session  
Host\Security\Require user authentication for remote connections by using  
Network Level Authentication
```

Note: This Group Policy path is provided by the Group Policy template **TerminalServer.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In the Microsoft Windows Vista Administrative Templates, this setting was initially named *Require user authentication using RDP 6.0 for remote connections*, but it was renamed starting with the Windows Server 2008 (non-R2) Administrative Templates.

Default Value:

Windows Server 2008 R2 or older: Disabled.

Windows Server 2012 (non-R2) or newer: Enabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●

18.10.56.3.9.5 Ensure 'Set client connection encryption level' is set to 'Enabled: High Level' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting specifies whether to require the use of a specific encryption level to secure communications between client computers and RD Session Host servers during Remote Desktop Protocol (RDP) connections. This policy only applies when you are using native RDP encryption. However, native RDP encryption (as opposed to SSL encryption) is not recommended. This policy does not apply to SSL encryption.

The recommended state for this setting is: **Enabled: High Level**.

Rationale:

If Remote Desktop client connections that use low level encryption are allowed, it is more likely that an attacker will be able to decrypt any captured Remote Desktop Services network traffic.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **3**.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal  
Services:MinEncryptionLevel
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled: High Level**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Remote Desktop Services\Remote Desktop Session Host\Security\Set  
client connection encryption level
```

Note: This Group Policy path is provided by the Group Policy template **TerminalServer.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Enabled: High Level. (All communications between clients and RD Session Host servers during remote connections using native RDP encryption must be 128-bit strength. Clients that do not support 128-bit encryption will be unable to establish Remote Desktop Server sessions.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224948
Rule ID: SV-224948r877394_rule
STIG ID: WN16-CC-000410
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			

18.10.56.3.10 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.

18.10.56.3.10.1 Ensure 'Set time limit for active but idle Remote Desktop Services sessions' is set to 'Enabled: 15 minutes or less, but not Never (0)' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting allows you to specify the maximum amount of time that an active Remote Desktop Services session can be idle (without user input) before it is automatically disconnected.

The recommended state for this setting is: **Enabled: 15 minutes or less, but not Never (0)**.

Rationale:

This setting helps to prevent active Remote Desktop sessions from tying up the computer for long periods of time while not in use, preventing computing resources from being consumed by large numbers of inactive sessions. In addition, old, forgotten Remote Desktop sessions that are still active can cause password lockouts if the user's password has changed but the old session is still running. For systems that limit the number of connected users (e.g. servers in the default Administrative mode - 2 sessions only), other users' old but still active sessions can prevent another user from connecting, resulting in an effective denial of service.

In addition, session timeouts that are misconfigured or set for a long period of time can leave the system open to an attacker hijacking the session.

Impact:

Remote Desktop Services will automatically disconnect active but idle sessions after 15 minutes (or the specified amount of time). The user receives a warning two minutes before the session disconnects, which allows the user to press a key or move the mouse to keep the session active. Note that idle session time limits do not apply to console sessions.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a REG_DWORD value of **900000** or less, but not **0**

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal  
Services:MaxIdleTime
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled: 15 minutes or less, but not Never (0)**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Remote Desktop Services\Remote Desktop Session Host\Session Time  
Limits\Set time limit for active but idle Remote Desktop Services sessions
```

Note: This Group Policy path is provided by the Group Policy template **TerminalServer.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was named *Set time limit for active but idle Terminal Services sessions*, but it was renamed starting with the Windows 7 & Server 2008 R2 Administrative Templates.

Default Value:

Disabled. (Remote Desktop Services allows sessions to remain active but idle for an unlimited amount of time.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	16.11 <u>Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

18.10.56.3.10.2 Ensure 'Set time limit for disconnected sessions' is set to 'Enabled: 1 minute' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting allows you to configure a time limit for disconnected Remote Desktop Services sessions.

The recommended state for this setting is: **Enabled: 1 minute**.

Rationale:

This setting helps to prevent active Remote Desktop sessions from tying up the computer for long periods of time while not in use, preventing computing resources from being consumed by large numbers of disconnected but still active sessions. In addition, old, forgotten Remote Desktop sessions that are still active can cause password lockouts if the user's password has changed but the old session is still running. For systems that limit the number of connected users (e.g. servers in the default Administrative mode - 2 sessions only), other users' old but still active sessions can prevent another user from connecting, resulting in an effective denial of service. This setting is important to ensure a disconnected session is properly terminated.

In addition, session timeouts that are misconfigured or set for a long period of time can leave the system open to an attacker hijacking the session.

Impact:

Disconnected Remote Desktop sessions are deleted from the server after 1 minute. Note that disconnected session time limits do not apply to console sessions.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **60000**.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal  
Services:MaxDisconnectionTime
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled: 1 minute**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Remote Desktop Services\Remote Desktop Session Host\Session Time  
Limits\Set time limit for disconnected sessions
```

Note: This Group Policy path is provided by the Group Policy template **TerminalServer.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Disconnected Remote Desktop sessions are maintained for an unlimited time on the server.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	16.11 <u>Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

18.10.56.3.11 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.

18.10.56.3.11.1 Ensure 'Do not delete temp folders upon exit' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting specifies whether Remote Desktop Services retains a user's per-session temporary folders at logoff.

The recommended state for this setting is: **Disabled**.

Rationale:

Sensitive information could be contained inside the temporary folders and visible to other administrators that log into the system.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal  
Services>DeleteTempDirsOnExit
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Remote Desktop Services\Remote Desktop Session Host\Temporary  
Folders\Do not delete temp folders upon exit
```

Note: This Group Policy path is provided by the Group Policy template **TerminalServer.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was named *Do not delete temp folder upon exit*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Default Value:

Disabled. (Temporary folders are deleted when a user logs off.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.4 <u>Enforce Data Retention</u> Retain data according to the enterprise's data management process. Data retention must include both minimum and maximum timelines.			

18.10.56.3.11.2 Ensure 'Do not use temporary folders per session' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

By default, Remote Desktop Services creates a separate temporary folder on the RD Session Host server for each active session that a user maintains on the RD Session Host server. The temporary folder is created on the RD Session Host server in a Temp folder under the user's profile folder and is named with the **sessionid**. This temporary folder is used to store individual temporary files.

To reclaim disk space, the temporary folder is deleted when the user logs off from a session.

The recommended state for this setting is: **Disabled**.

Rationale:

Disabling this setting keeps the cached data independent for each session, both reducing the chance of problems from shared cached data between sessions, and keeping possibly sensitive data separate to each user session.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal  
Services:PerSessionTempDir
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Remote Desktop Services\Remote Desktop Session Host\Temporary  
Folders\Do not use temporary folders per session
```

Note: This Group Policy path is provided by the Group Policy template **TerminalServer.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Per-session temporary folders are created.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.4 <u>Enforce Data Retention</u> Retain data according to the enterprise's data management process. Data retention must include both minimum and maximum timelines.			

18.10.57 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.

18.10.57.1 Ensure 'Prevent downloading of enclosures' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting prevents the user from having enclosures (file attachments) downloaded from an RSS feed to the user's computer.

The recommended state for this setting is: **Enabled**.

Rationale:

Allowing attachments to be downloaded through the RSS feed can introduce files that could have malicious intent.

Impact:

Users cannot set the Feed Sync Engine to download an enclosure through the Feed property page. Developers cannot change the download setting through feed APIs.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Internet  
Explorer\Feeds:DisableEnclosureDownload
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

Computer Configuration\Policies\Administrative Templates\Windows Components\RSS Feeds\Prevent downloading of enclosures

Note: This Group Policy path is provided by the Group Policy template **InetRes.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was named *Turn off downloading of enclosures*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Default Value:

Disabled. (Users can set the Feed Sync Engine to download an enclosure through the Feed property page. Developers can change the download setting through the Feed APIs.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224949
Rule ID: SV-224949r569186_rule
STIG ID: WN16-CC-000420
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.			
v7	7.2 Disable Unnecessary or Unauthorized Browser or Email Client Plugins Uninstall or disable any unauthorized browser or email client plugins or add-on applications.			

18.10.57.2 Ensure 'Turn on Basic feed authentication over HTTP' is set to 'Not configured' or 'Disabled' (STIG only) (Automated)

Profile Applicability:

- STIG Member Server
- STIG Domain Controller

Description:

This policy setting allows users to have their feeds authenticated through the Basic authentication scheme over an unencrypted HTTP connection.

The recommended STIG state for this setting is: **Not configured** or **Disabled**.

Rationale:

Basic authentication uses plain-text passwords that could be used to compromise a system. Disabling Basic authentication will reduce this potential.

Impact:

Plain-text passwords for RSS feeds over HTTP will not be allowed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0** or that **no value exists**.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Feeds:AllowBasicAuthInClear
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Not configured** or **Disabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\RSS Feeds\Turn on Basic feed authentication over HTTP
```

Note: This Group Policy path is provided by the Group Policy template **InetRes.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Windows RSS Platform does not authenticate feeds to servers by using the Basic authentication scheme in combination with a less secure HTTP connection.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224951
Rule ID: SV-224951r569186_rule
STIG ID: WN16-CC-000430
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.4 <u>Restrict Unnecessary or Unauthorized Browser and Email Client Extensions</u> Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.			
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.			

18.10.58 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.

18.10.58.1 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.

18.10.58.2 Ensure 'Allow Cloud Search' is set to 'Enabled: Disable Cloud Search' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting allows search and Cortana to search cloud sources like OneDrive and SharePoint.

The recommended state for this setting is: **Enabled: Disable Cloud Search**.

Rationale:

Due to privacy concerns, data should never be sent to any third-party since this data could contain sensitive information.

Impact:

Search and Cortana will not be permitted to search cloud sources like OneDrive and SharePoint.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Windows Search:AllowCloudSearch
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled: Disable Cloud Search**:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Search\Allow Cloud Search
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **Search.admx/adml** that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Default Value:

Enabled: Enable Cloud Search. (Allow search and Cortana to search cloud sources like OneDrive and SharePoint.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.10.58.3 Ensure 'Allow indexing of encrypted files' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting controls whether encrypted items are allowed to be indexed. When this setting is changed, the index is rebuilt completely. Full volume encryption (such as BitLocker Drive Encryption or a non-Microsoft solution) must be used for the location of the index to maintain security for encrypted files.

The recommended state for this setting is: **Disabled**.

Rationale:

Indexing and allowing users to search encrypted files could potentially reveal confidential data stored within the encrypted files.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Windows  
Search:AllowIndexingEncryptedStoresOrItems
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Search\Allow indexing of encrypted files
```

Note: This Group Policy path is provided by the Group Policy template **Search.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Search service components (including non-Microsoft components) are expected not to index encrypted items or encrypted stores.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224952
Rule ID: SV-224952r569186_rule
STIG ID: WN16-CC-000440
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	14.8 <u>Encrypt Sensitive Information at Rest</u> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			

18.10.58.4 Ensure 'Allow search highlights' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting controls search highlights in the start menu search box and in search home.

The recommended state for this setting is: **Disabled**.

Rationale:

In a high security environment, data should never be sent to or received by any third-party since this data could contain sensitive information.

Impact:

“Interesting”, “informative”, and “noteworthy” information about the current date will not be displayed (by Microsoft) to the user.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Windows  
Search:EnableDynamicContentInWSB
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Search\Allow search highlights
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **Search.admx/adml** that is included with the Microsoft Windows 10 Release 21H2 Administrative Templates (or newer).

Default Value:

Enabled. (Search highlights in the start menu search box and in search home will be available.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			

18.10.59 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.

18.10.60 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.

18.10.61 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.

18.10.62 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).

18.10.62.1 Ensure 'Turn off KMS Client Online AVS Validation' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

The Key Management Service (KMS) is a Microsoft license activation method that entails setting up a local server to store the software licenses. The KMS server itself needs to connect to Microsoft to activate the KMS service, but subsequent on-network clients can activate Microsoft Windows OS and/or their Microsoft Office via the KMS server instead of connecting directly to Microsoft. This policy setting lets you opt-out of sending KMS client activation data to Microsoft automatically.

The recommended state for this setting is: **Enabled**.

Rationale:

Even though the KMS licensing method does not *require* KMS clients to connect to Microsoft, they still send KMS client activation state data to Microsoft automatically. Preventing this information from being sent can help reduce privacy concerns in high security environments.

Impact:

The computer is prevented from sending data to Microsoft regarding its KMS client activation state.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\CurrentVersion\Software  
Protection Platform:NoGenTicket
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Software Protection Platform\Turn off KMS Client Online AVS  
Validation
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **AVSValidationGP.admx/adml** that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

Default Value:

Disabled. (KMS client activation data will automatically be sent to Microsoft when the device activates.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

18.10.63 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.

18.10.64 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).

18.10.65 Store

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template [WinStoreUI.admx/adml](#) that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates, or by the Group Policy template [WindowsStore.admx/adml](#) that is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).

18.10.66 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).

18.10.67 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.

18.10.68 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.

18.10.69 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).

18.10.70 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.

18.10.71 Widgets

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template [NewsAndInterests.admx/adml](#) that is included with the Microsoft Windows 11 Release 21H2 Administrative Templates (or newer).

18.10.72 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.

18.10.73 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.

18.10.74 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.

18.10.75 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).

18.10.75.1 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).

18.10.75.2 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).

18.10.75.2.1 Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled: Warn and prevent bypass' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to manage the behavior of Windows SmartScreen. Windows SmartScreen helps keep PCs safer by warning users before running unrecognized programs downloaded from the Internet. Some information is sent to Microsoft about files and programs run on PCs with this feature enabled.

The recommended state for this setting is: **Enabled: Warn and prevent bypass**.

Rationale:

Windows SmartScreen helps keep PCs safer by warning users before running unrecognized programs downloaded from the Internet. However, due to the fact that some information is sent to Microsoft about files and programs run on PCs some organizations may prefer to disable it.

Impact:

Users will be warned and prevented from running unrecognized programs downloaded from the Internet.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1** (EnableSmartScreen) and **REG_SZ** value of **Block** (ShellSmartScreenLevel).

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System:EnableSmartScreen
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System:ShellSmartScreenLevel
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled: Warn and prevent bypass**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Windows Defender SmartScreen\Explorer\Configure Windows Defender  
SmartScreen
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **WindowsExplorer.admx/adml** that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Configure Windows SmartScreen*, but it was renamed starting with the Windows 10 Release 1703 Administrative Templates.

Default Value:

Disabled. (Windows SmartScreen behavior is managed by administrators on the PC by using Windows SmartScreen Settings in Action Center.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 <u>Enable Anti-Exploitation Features</u> Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.			
v7	8.3 <u>Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies</u> Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.			

18.10.75.2.2 Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled' (STIG only) (Automated)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting allows you to manage the behavior of Windows SmartScreen. Windows SmartScreen helps keep PCs safer by warning users before running unrecognized programs downloaded from the Internet. Some information is sent to Microsoft about files and programs run on PCs with this feature enabled.

The recommended STIG state for this setting is: **Enabled**.

The CIS recommended state for this setting is: **Enabled: Warn and prevent bypass**.

Note: The Server 2016 STIG does not specify which option to choose **Warn** or **Warn and prevent bypass**. The default value when enabling this policy is **Warn and prevent bypass**.

Rationale:

Windows SmartScreen helps keep PCs safer by warning users before running unrecognized programs downloaded from the Internet. However, due to the fact that some information is sent to Microsoft about files and programs run on PCs some organizations may prefer to disable it.

Impact:

Users will be warned before they are allowed to run unrecognized programs downloaded from the Internet.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1** (EnableSmartScreen) and **REG_SZ** value of **Block** or **Warn** (ShellSmartScreenLevel).

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System:EnableSmartScreen
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System:ShellSmartScreenLevel
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled: Warn and prevent bypass**:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender SmartScreen\Explorer\Configure Windows Defender SmartScreen
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **WindowsExplorer.admx/adml** that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Configure Windows SmartScreen*, but it was renamed starting with the Windows 10 Release 1703 Administrative Templates.

Default Value:

Disabled. (Windows SmartScreen behavior is managed by administrators on the PC by using Windows SmartScreen Settings in Action Center.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224940
Rule ID: SV-224940r569186_rule
STIG ID: WN16-CC-000330
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 <u>Enable Anti-Exploitation Features</u> Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.			
v7	8.3 <u>Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies</u> Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.			

18.10.76 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.

18.10.77 Windows Game Recording and Broadcasting

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template **GameDVR.admx/adml** that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

18.10.78 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.

18.10.79 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).

18.10.79.1 Ensure 'Allow suggested apps in Windows Ink Workspace' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting determines whether suggested apps in Windows Ink Workspace are allowed.

The recommended state for this setting is: **Disabled**.

Rationale:

This Microsoft feature is designed to collect data and suggest apps based on that data collected. Disabling this setting will help ensure your data is not shared with any third party.

Impact:

The suggested apps in Windows Ink Workspace will not be allowed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\WindowsInkWorkspace:AllowSuggestedAppsInWindowsInkWorkspace
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Ink Workspace\Allow suggested apps in Windows Ink Workspace
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **WindowsInkWorkspace.admx/adml** that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

Default Value:

Enabled. (The suggested apps in Windows Ink Workspace will be allowed.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.10.79.2 Ensure 'Allow Windows Ink Workspace' is set to 'Enabled: On, but disallow access above lock' OR 'Enabled: Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether Windows Ink items are allowed above the lock screen.

The recommended state for this setting is: **Enabled: On, but disallow access above lock** OR **Enabled: Disabled**.

Rationale:

Allowing any apps to be accessed while system is locked is not recommended. If this feature is permitted, it should only be accessible once a user authenticates with the proper credentials.

Impact:

Windows Ink Workspace will not be permitted above the lock screen.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0** or **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\WindowsInkWorkspace:AllowWindowsInkWorkspace
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled: On, but disallow access above lock** OR **Enabled: Disabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Windows Ink Workspace\Allow Windows Ink Workspace
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **WindowsInkWorkspace.admx/adml** that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

Default Value:

Enabled. (Windows Ink Workspace is permitted above the lock screen.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.10.80 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.

18.10.80.1 Ensure 'Allow user control over installs' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This setting controls whether users are permitted to change installation options that typically are available only to system administrators. The security features of Windows Installer normally prevent users from changing installation options that are typically reserved for system administrators, such as specifying the directory to which files are installed. If Windows Installer detects that an installation package has permitted the user to change a protected option, it stops the installation and displays a message. These security features operate only when the installation program is running in a privileged security context in which it has access to directories denied to the user.

The recommended state for this setting is: **Disabled**.

Rationale:

In an enterprise managed environment, only IT staff with administrative rights should be installing or changing software on a system. Allowing users the ability to have any control over installs can risk unapproved software from being installed or removed from a system, which could cause the system to become vulnerable to compromise.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer:EnableUserControl
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Windows Installer\Allow user control over installs
```

Note: This Group Policy path is provided by the Group Policy template **MSI.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was named *Enable user control over installs*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Default Value:

Disabled. (The security features of Windows Installer will prevent users from changing installation options typically reserved for system administrators, such as specifying the directory to which files are installed.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224953
Rule ID: SV-224953r852334_rule
STIG ID: WN16-CC-000450
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

18.10.80.2 Ensure 'Always install with elevated privileges' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This setting controls whether or not Windows Installer should use system permissions when it installs any program on the system.

Note: This setting appears both in the Computer Configuration and User Configuration folders. To make this setting effective, you must enable the setting in both folders.

Caution: If enabled, skilled users can take advantage of the permissions this setting grants to change their privileges and gain permanent access to restricted files and folders. Note that the User Configuration version of this setting is not guaranteed to be secure.

The recommended state for this setting is: **Disabled**.

Rationale:

Users with limited privileges can exploit this feature by creating a Windows Installer installation package that creates a new local account that belongs to the local built-in Administrators group, adds their current account to the local built-in Administrators group, installs malicious software, or performs other unauthorized activities.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer:AlwaysInstallElevated
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Installer\Always install with elevated privileges

Note: This Group Policy path is provided by the Group Policy template **MSI.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Windows Installer will apply the current user's permissions when it installs programs that a system administrator does not distribute or offer. This will prevent standard users from installing applications that affect system-wide configuration items.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224954
Rule ID: SV-224954r852335_rule
STIG ID: WN16-CC-000460
Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	4.3 <u>Ensure the Use of Dedicated Administrative Accounts</u> Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●

18.10.80.3 Ensure 'Prevent Internet Explorer security prompt for Windows Installer scripts' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting controls whether Web-based programs are allowed to install software on the computer without notifying the user.

The recommended state for this setting is: **Disabled**.

Rationale:

Suppressing the system warning can pose a security risk and increase the attack surface on the system.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer:SafeForScripting
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Windows Installer\Prevent Internet Explorer security prompt for  
Windows Installer scripts
```

Note: This Group Policy path is provided by the Group Policy template **MSI.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Disable IE security prompt for Windows Installer scripts*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Default Value:

Disabled. (When a script hosted by an Internet browser tries to install a program on the system, the system warns users and allows them to select or refuse the installation.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224955
Rule ID: SV-224955r569186_rule
STIG ID: WN16-CC-000470
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.5 <u>Allowlist Authorized Software</u> Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.			

18.10.81 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.

18.10.81.1 Ensure 'Sign-in and lock last interactive user automatically after a restart' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting controls whether a device will automatically sign-in the last interactive user after Windows Update restarts the system.

The recommended state for this setting is: **Disabled**.

Rationale:

Disabling this feature will prevent the caching of user's credentials and unauthorized use of the device, and also ensure the user is aware of the restart.

Impact:

The device does not store the user's credentials for automatic sign-in after a Windows Update restart. The users' lock screen apps are not restarted after the system restarts. The user is required to present the logon credentials in order to proceed after restart.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:DisableAutomaticRestartSignOn
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Windows Logon Options\Sign-in and lock last interactive user  
automatically after a restart
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **WinLogon.admx/adml** that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Sign-in last interactive user automatically after a system-initiated restart*, but it was renamed starting with the Windows 10 Release 1903 Administrative Templates.

Default Value:

Enabled. (The device securely saves the user's credentials (including the user name, domain and encrypted password) to configure automatic sign-in after a Windows Update restart. After the Windows Update restart, the user is automatically signed-in and the session is automatically locked with all the lock screen apps configured for that user.)

Additional Information:

Disable this policy setting so that the device does not store the user's credentials for automatic sign-in after a Windows Update restart and the users' lock screen apps are not restarted after the system restarts.

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224956
Rule ID: SV-224956r877377_rule
STIG ID: WN16-CC-000480
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	16.11 <u>Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

18.10.82 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.

18.10.83 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.

18.10.84 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.

18.10.85 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.

18.10.86 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).

18.10.86.1 Ensure 'Turn on PowerShell Script Block Logging' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting enables logging of all PowerShell script input to the **Applications and Services Logs\Microsoft\Windows\PowerShell\Operational** Event Log channel.

The recommended state for this setting is: **Enabled**.

Note: If logging of *Script Block Invocation Start/Stop Events* is enabled (option box checked), PowerShell will log additional events when invocation of a command, script block, function, or script starts or stops. Enabling this option generates a high volume of event logs. CIS has intentionally chosen not to make a recommendation for this option, since it generates a large volume of events. **If an organization chooses to enable the optional setting (checked), this also conforms to the benchmark.**

Rationale:

Logs of PowerShell script input can be very valuable when performing forensic investigations of PowerShell attack incidents to determine what occurred.

Impact:

PowerShell script input will be logged to the **Applications and Services Logs\Microsoft\Windows\PowerShell\Operational** Event Log channel, which can contain credentials and sensitive information.

Note: Configuring this setting to **Enabled** generates a high volume of event logs which will be overwritten if the log size is not expanded or offloaded to a log collection system.

Warning: There are potential risks of capturing credentials and sensitive information in the PowerShell logs, which could be exposed to users who have read-access to those logs. Microsoft provides a feature called "Protected Event Logging" to better secure event log data. For assistance with protecting event logging, visit: [About Logging Windows - PowerShell | Microsoft Docs](#).

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging:EnableScriptBlockLogging
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows PowerShell\Turn on PowerShell Script Block Logging
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **PowerShellExecutionPolicy.admx/adml** that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

Default Value:

Enabled. (PowerShell will log script blocks the first time they are used.)

References:

1. https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_logging_windows?view=powershell-7.2#protected-event-logging

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224957
Rule ID: SV-224957r569186_rule
STIG ID: WN16-CC-000490
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.8 <u>Collect Command-Line Audit Logs</u> Collect command-line audit logs. Example implementations include collecting audit logs from PowerShell®, BASH™, and remote administrative terminals.			
v7	8.8 <u>Enable Command-line Audit Logging</u> Enable command-line audit logging for command shells, such as Microsoft Powershell and Bash.			

18.10.86.2 Ensure 'Turn on PowerShell Transcription' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This Policy setting lets you capture the input and output of Windows PowerShell commands into text-based transcripts.

The recommended state for this setting is: **Enabled**.

Rationale:

PowerShell transcript input can be very valuable when performing forensic investigations of PowerShell attack incidents to determine what occurred.

Impact:

PowerShell transcript input will be logged to **PowerShell_transcript** output files, which are saved to the My Documents folder (within a separate subfolder for each day) of each users' profile by default. Optionally, a specific output directory name can be specified, which will contain all PowerShell transcript logs in a subfolder of My Documents. If specifying a full path outside the users My Documents folder, other users on the system could have access to view these logs, which may contain sensitive information such as passwords.

Warning: There are potential risks of capturing credentials and sensitive information in **PowerShell_transcript** output files, which could be exposed to users who have read access to the files.

Warning #2: PowerShell Transcription is not compatible with the natively installed PowerShell v4 on Microsoft Windows 10 Release 1511 and Server 2012 R2 and below. If this recommendation is set as prescribed, PowerShell will need to be updated to at least v5.1 or newer. For more information on updating PowerShell, please see [Windows PowerShell System Requirements - PowerShell | Microsoft Learn](#).

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\PowerShell\Transcription:EnableTranscription
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows PowerShell\Turn on PowerShell Transcription
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **PowerShellExecutionPolicy.admx/adml** that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

Default Value:

Disabled. (Transcription of PowerShell-based applications is disabled by default, although transcription can still be enabled through the **Start-Transcript** cmdlet.)

References:

1. https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_group_policy_settings?view=powershell-7.2#turn-on-powershell-transcription

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-257502
Rule ID: SV-257502r921892_rule
STIG ID: WN16-CC-000555
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.8 Collect Command-Line Audit Logs Collect command-line audit logs. Example implementations include collecting audit logs from PowerShell®, BASH™, and remote administrative terminals.		●	●

18.10.87 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).

18.10.88 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.

18.10.88.1 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.

18.10.88.1.1 Ensure 'Allow Basic authentication' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting allows you to manage whether the Windows Remote Management (WinRM) client uses Basic authentication.

The recommended state for this setting is: **Disabled**.

Rationale:

Basic authentication is less robust than other authentication methods available in WinRM because credentials including passwords are transmitted in plain text. An attacker who is able to capture packets on the network where WinRM is running may be able to determine the credentials used for accessing remote hosts via WinRM.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\WinRM\Client:AllowBasic
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Windows Remote Management (WinRM)\WinRM Client\Allow Basic  
authentication
```

Note: This Group Policy path is provided by the Group Policy template **WindowsRemoteManagement.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (The WinRM client does not use Basic authentication.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224958
Rule ID: SV-224958r877395_rule
STIG ID: WN16-CC-000500
Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	16.5 <u>Encrypt Transmittal of Username and Authentication Credentials</u> Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.			

18.10.88.1.2 Ensure 'Allow unencrypted traffic' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting allows you to manage whether the Windows Remote Management (WinRM) client sends and receives unencrypted messages over the network.

The recommended state for this setting is: **Disabled**.

Rationale:

Encrypting WinRM network traffic reduces the risk of an attacker viewing or modifying WinRM messages as they transit the network.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\WinRM\Client:AllowUnencryptedTraffic
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Windows Remote Management (WinRM)\WinRM Client\Allow unencrypted  
traffic
```

Note: This Group Policy path is provided by the Group Policy template **WindowsRemoteManagement.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (The WinRM client sends or receives only encrypted messages over the network.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224959
Rule ID: SV-224959r877382_rule
STIG ID: WN16-CC-000510
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.			

18.10.88.1.3 Ensure 'Disallow Digest authentication' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting allows you to manage whether the Windows Remote Management (WinRM) client will not use Digest authentication.

The recommended state for this setting is: **Enabled**.

Rationale:

Digest authentication is less robust than other authentication methods available in WinRM, an attacker who is able to capture packets on the network where WinRM is running may be able to determine the credentials used for accessing remote hosts via WinRM.

Impact:

The WinRM client will not use Digest authentication.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\WinRM\Client:AllowDigest
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Windows Remote Management (WinRM)\WinRM Client\Disallow Digest  
authentication
```

Note: This Group Policy path is provided by the Group Policy template **WindowsRemoteManagement.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (The WinRM client will use Digest authentication.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224960
Rule ID: SV-224960r877395_rule
STIG ID: WN16-CC-000520
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	16.5 <u>Encrypt Transmittal of Username and Authentication Credentials</u> Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.			

18.10.88.2 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.

18.10.88.2.1 Ensure 'Allow Basic authentication' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting allows you to manage whether the Windows Remote Management (WinRM) service accepts Basic authentication from a remote client.

The recommended state for this setting is: **Disabled**.

Rationale:

Basic authentication is less robust than other authentication methods available in WinRM because credentials including passwords are transmitted in plain text. An attacker who is able to capture packets on the network where WinRM is running may be able to determine the credentials used for accessing remote hosts via WinRM.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\WinRM\Service:AllowBasic
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Windows Remote Management (WinRM)\WinRM Service\Allow Basic  
authentication
```

Note: This Group Policy path is provided by the Group Policy template **WindowsRemoteManagement.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (The WinRM service will not accept Basic authentication from a remote client.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224961
Rule ID: SV-224961r877395_rule
STIG ID: WN16-CC-000530
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	16.5 <u>Encrypt Transmittal of Username and Authentication Credentials</u> Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.			

18.10.88.2.2 Ensure 'Allow remote server management through WinRM' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting allows you to manage whether the Windows Remote Management (WinRM) service automatically listens on the network for requests on the HTTP transport over the default HTTP port.

The recommended state for this setting is: **Disabled**.

Rationale:

Any feature is a potential avenue of attack, those that enable inbound network connections are particularly risky. Only enable the use of the Windows Remote Management (WinRM) service on trusted networks and when feasible employ additional controls such as IPsec.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\WinRM\Service:AllowAutoConfig
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service\Allow remote server management through WinRM
```

Note: This Group Policy path is provided by the Group Policy template **WindowsRemoteManagement.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Allow automatic configuration of listeners*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Default Value:

Disabled. (The WinRM service will not respond to requests from a remote computer, regardless of whether or not any WinRM listeners are configured.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

18.10.88.2.3 Ensure 'Allow unencrypted traffic' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting allows you to manage whether the Windows Remote Management (WinRM) service sends and receives unencrypted messages over the network.

The recommended state for this setting is: **Disabled**.

Rationale:

Encrypting WinRM network traffic reduces the risk of an attacker viewing or modifying WinRM messages as they transit the network.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\WinRM\Service:AllowUnencryptedTraffic
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service\Allow unencrypted traffic
```

Note: This Group Policy path is provided by the Group Policy template **WindowsRemoteManagement.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (The WinRM service sends or receives only encrypted messages over the network.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224962
Rule ID: SV-224962r877382_rule
STIG ID: WN16-CC-000540
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.			

18.10.88.2.4 Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting allows you to manage whether the Windows Remote Management (WinRM) service will allow RunAs credentials to be stored for any plug-ins.

The recommended state for this setting is: **Enabled**.

Note: If you enable and then disable this policy setting, any values that were previously configured for **RunAsPassword** will need to be reset.

Rationale:

Although the ability to store RunAs credentials is a convenient feature it increases the risk of account compromise slightly. For example, if you forget to lock your desktop before leaving it unattended for a few minutes another person could access not only the desktop of your computer but also any hosts you manage via WinRM with cached RunAs credentials.

Impact:

The WinRM service will not allow the **RunAsUser** or **RunAsPassword** configuration values to be set for any plug-ins. If a plug-in has already set the **RunAsUser** and **RunAsPassword** configuration values, the **RunAsPassword** configuration value will be erased from the credential store on the computer.

If this setting is later Disabled again, any values that were previously configured for **RunAsPassword** will need to be reset.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\WinRM\Service:DisableRunAs
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Windows Remote Management (WinRM)\WinRM Service\Disallow WinRM  
from storing RunAs credentials
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **WindowsRemoteManagement.admx/adml** that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (The WinRM service will allow the **RunAsUser** and **RunAsPassword** configuration values to be set for plug-ins and the **RunAsPassword** value will be stored securely.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224963
Rule ID: SV-224963r852338_rule
STIG ID: WN16-CC-000550
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	14.3 <u>Disable Workstation to Workstation Communication</u> Disable all workstation to workstation communication to limit an attacker's ability to move laterally and compromise neighboring systems, through technologies such as Private VLANs or microsegmentation.		●	●

18.10.89 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.

18.10.89.1 Ensure 'Allow Remote Shell Access' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting allows you to manage configuration of remote access to all supported shells to execute scripts and commands.

The recommended state for this setting is: **Disabled**.

Note: The GPME help text for this setting is incorrectly worded, implying that configuring it to **Enabled** will reject new Remote Shell connections, and setting it to **Disabled** will allow Remote Shell connections. The opposite is true (and is consistent with the title of the setting). This is a wording mistake by Microsoft in the Administrative Template.

Rationale:

Any feature is a potential avenue of attack, those that enable inbound network connections are particularly risky. Only enable the use of the Windows Remote Shell on trusted networks and when feasible employ additional controls such as IPsec.

Impact:

New Remote Shell connections are not allowed and are rejected by the server.

Note: On Server 2012 (non-R2) or newer, due to design changes in the OS after Server 2008 R2, configuring this setting as prescribed will prevent the ability to add or remove Roles and Features (even locally) via the GUI. We therefore recommend that the necessary Roles and Features be installed prior to configuring this setting on a Level 2 server. Alternatively, Roles and Features can still be added or removed using the PowerShell commands **Add-WindowsFeature** or **Remove-WindowsFeature** in the Server Manager module, even with this setting configured.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

HKLM\SOFTWARE\Policies\Microsoft\Windows\WinRM\Service\WinRS:AllowRemoteShell Access

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Shell\Allow Remote Shell Access

Note: This Group Policy path is provided by the Group Policy template **WindowsRemoteShell.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Enabled. (New Remote Shell connections are allowed.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

18.10.90 Windows Sandbox

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template [WindowsSandbox.admx/adml](#) that is included with the Microsoft Windows 11 Release 21H2 Administrative Templates (or newer).

18.10.91 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.

18.10.91.1 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).

18.10.91.2 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).

18.10.91.2.1 Ensure 'Prevent users from modifying settings' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting prevent users from making changes to the Exploit protection settings area in the Windows Security settings.

The recommended state for this setting is: **Enabled**.

Rationale:

Only authorized IT staff should be able to make changes to the exploit protection settings in order to ensure the organizations specific configuration is not modified.

Impact:

Local users cannot make changes in the Exploit protection settings area.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender Security Center\App and Browser protection:DisallowExploitProtectionOverride
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Security\App and browser protection\Prevent users from modifying settings
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **WindowsDefenderSecurityCenter.admx/adml** that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Default Value:

Disabled. (Local users are allowed to make changes in the Exploit protection settings area.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 <u>Enable Anti-Exploitation Features</u> Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.			
v7	8.3 <u>Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies</u> Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.			

18.10.92 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.

18.10.92.1 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).

18.10.92.1.1 Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting specifies that Automatic Updates will wait for computers to be restarted by the users who are logged on to them to complete a scheduled installation.

The recommended state for this setting is: **Disabled**.

Note: This setting applies only when you configure Automatic Updates to perform scheduled update installations. If you configure the Configure Automatic Updates setting to Disabled, this setting has no effect.

Rationale:

Some security updates require that the computer be restarted to complete an installation. If the computer cannot restart automatically, then the most recent update will not completely install and no new updates will download to the computer until it is restarted. Without the auto-restart functionality, users who are not security-conscious may choose to indefinitely delay the restart, therefore keeping the computer in a less secure state.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU:NoAutoRebootWithLoggedOnUsers
```


Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Windows Update\Legacy Policies\No auto-restart with logged on  
users for scheduled automatic updates installations
```

Note: This Group Policy path is provided by the Group Policy template **WindowsUpdate.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *No auto-restart for scheduled Automatic Updates installations*, but it was renamed starting with the Windows 7 & Server 2008 R2 Administrative Templates.

Default Value:

Disabled. (Automatic Updates will notify the user that the computer will automatically restart in 5 minutes to complete the installation of security updates.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>7.3 Perform Automated Operating System Patch Management</u> Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v7	<u>3.4 Deploy Automated Operating System Patch Management Tools</u> Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.			

18.10.92.2 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).

18.10.92.2.1 Ensure 'Configure Automatic Updates' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting specifies whether computers in your environment will receive security updates from Windows Update or WSUS. If you configure this policy setting to Enabled, the operating system will recognize when a network connection is available and then use the network connection to search Windows Update or your designated intranet site for updates that apply to them.

After you configure this policy setting to Enabled, select one of the following three options in the Configure Automatic Updates Properties dialog box to specify how the service will work:

- 2 - Notify for download and auto install (*Notify before downloading any updates*)
- 3 - Auto download and notify for install (*Download the updates automatically and notify when they are ready to be installed.*) (Default setting)
- 4 - Auto download and schedule the install (*Automatically download updates and install them on the schedule specified below.*)
- 5 - Allow local admin to choose setting (*Leave decision on above choices up to the local Administrators (Not Recommended)*)

The recommended state for this setting is: **Enabled**.

Note: The sub-setting "Configure automatic updating:" has 4 possible values – all of them are valid depending on specific organizational needs, however if feasible we suggest using a value of **4 - Auto download and schedule the install**. This suggestion is not a scored requirement.

Note #2: Organizations that utilize a third-party solution for patching may choose to exempt themselves from this recommendation, and instead configure it to **Disabled** so that the native Windows Update mechanism does not interfere with the third-party patching process.

Rationale:

Although each version of Windows is thoroughly tested before release, it is possible that problems will be discovered after the products are shipped. The Configure Automatic Updates setting can help you ensure that the computers in your environment will always have the most recent critical operating system updates and service packs installed.

Impact:

Critical operating system updates and service packs will be installed as necessary.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU:NoAutoUpdate

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\Manage end user experience\Configure Automatic Updates

Note: This Group Policy path is provided by the Group Policy template **WindowsUpdate.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Enabled: 3 - Auto download and notify for install. (Windows finds updates that apply to the computer and downloads them in the background (the user is not notified or interrupted during this process). When the downloads are complete, users will be notified that they are ready to install. After going to Windows Update, users can install them.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.3 <u>Perform Automated Operating System Patch Management</u> Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v7	3.4 <u>Deploy Automated Operating System Patch Management Tools</u> Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.			

18.10.92.2.2 Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting specifies when computers in your environment will receive security updates from Windows Update or WSUS.

The recommended state for this setting is: **0 - Every day**.

Note: This setting is only applicable if **4 - Auto download and schedule the install** is selected in recommendation 'Configure Automatic Updates'. It will have no impact if any other option is selected.

Rationale:

Although each version of Windows is thoroughly tested before release, it is possible that problems will be discovered after the products are shipped. The Configure Automatic Updates setting can help you ensure that the computers in your environment will always have the most recent critical operating system updates and service packs installed.

Impact:

If **4 - Auto download and schedule the install** is selected in recommendation 'Configure Automatic Updates', critical operating system updates and service packs will automatically download every day (at 3:00 A.M., by default).

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU\ScheduledInstallDay

Remediation:

To establish the recommended configuration via GP, set the following UI path to **0 - Every day**:

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Windows Update\Manage end user experience\Configure Automatic  
Updates: Scheduled install day
```

Note: This Group Policy path is provided by the Group Policy template **WindowsUpdate.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Not Defined. (Since the default value of Configure Automatic Updates is **3 - Auto download and notify for install**, this setting is not applicable by default.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>7.3 Perform Automated Operating System Patch Management</u> Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v7	<u>3.4 Deploy Automated Operating System Patch Management Tools</u> Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.			

18.10.92.3 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).

18.10.92.4 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.

18.10.92.4.1 Ensure 'Manage preview builds' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting manages which updates that are received prior to the update being released.

Dev Channel: Ideal for highly technical users. Insiders in the Dev Channel will receive builds from our active development branch that is earliest in a development cycle. These builds are not matched to a specific Windows 10 release.

Beta Channel: Ideal for feature explorers who want to see upcoming Windows 10 features. Your feedback will be especially important here as it will help our engineers ensure key issues are fixed before a major release.

Release Preview Channel (default): Insiders in the Release Preview Channel will have access to the upcoming release of Windows 10 prior to it being released to the world. These builds are supported by Microsoft. The Release Preview Channel is where we recommend companies preview and validate upcoming Windows 10 releases before broad deployment within their organization.

The recommended state for this setting is: **Disabled**.

Note: Preview Build enrollment requires a telemetry level setting of 2 or higher and your domain registered on insider.windows.com. For additional information on Preview Builds, see: <https://aka.ms/wipforbiz>

Rationale:

It can be risky for experimental features to be allowed in an enterprise managed environment because this can introduce bugs and security holes into systems, making it easier for an attacker to gain access. It is generally preferred to only use production-ready builds.

Impact:

Preview builds are prevented from installing on the device.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\ManagePreviewBuildsPolicyValue
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\Manage updates offered from Windows Update\Manage preview builds
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **WindowsUpdate.admx/adml** that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Default Value:

Disabled. (Windows Update will not offer you any pre-release updates and you will receive such content once released to the world. Disabling this policy will cause any devices currently on a pre-release build to opt out and stay on the latest Feature Update once released.)

References:

1. <https://docs.microsoft.com/en-us/windows-insider/business/manage-builds>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.5 Allowlist Authorized Software Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.		●	●
v7	2.6 Address unapproved software Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●

18.10.92.4.2 Ensure 'Select when Preview Builds and Feature Updates are received' is set to 'Enabled: 180 or more days' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines when Preview Build or Feature Updates are received.

Defer Updates This enables devices to defer taking the next Feature Update available to your channel for up to 14 days for all the pre-release channels and up to 365 days for the Semi-Annual Channel. Or, if the device is updating from the Semi-Annual Channel, a version for the device to move to and/or stay on until the policy is updated or the device reaches end of service can be specified. Note: If you set both policies, the version specified will take precedence and the deferrals will not be in effect. Please see the Windows Release Information page for OS version information.

Pause Updates To prevent Feature Updates from being received on their scheduled time, you can temporarily pause Feature Updates. The pause will remain in effect for 35 days from the specified start date or until the field is cleared (Quality Updates will still be offered).

Note: If the "Allow Diagnostic Data" (formerly "Allow Telemetry") policy is set to 0, this policy will have no effect.

Note #2: Starting with Windows 10 R1607, Microsoft introduced a new Windows Update (WU) client behavior called **Dual Scan**, with an eye to cloud-based update management. In some cases, this Dual Scan feature can interfere with Windows Updates from Windows Server Update Services (WSUS) and/or manual WU updates. If you are using WSUS in your environment, you may need to set the above setting to **Not Configured** or configure the setting *Do not allow update deferral policies to cause scans against Windows Update* (added in the Windows 10 Release 1709 Administrative Templates) in order to prevent the Dual Scan feature from interfering. More information on Dual Scan is available at these links:

- [Demystifying "Dual Scan" – WSUS Product Team Blog](#)
- [Improving Dual Scan on 1607 – WSUS Product Team Blog](#)

Note #3: Prior to Windows 10 R1703, values above 180 days are not recognized by the OS. Starting with Windows 10 R1703, the maximum number of days you can defer is 365 days.

Rationale:

In a production environment, it is preferred to only use software and features that are publicly available, after they have gone through rigorous testing in beta.

Impact:

Feature Updates will be delayed until they are publicly released to general public by Microsoft.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1** (DeferFeatureUpdates) and **180** (DeferFeatureUpdatesPeriodInDays).

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate:DeferFeatureUpdates
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate:DeferFeatureUpdatesPeriodInDays
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled: 180 or more days**:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\Manage updates offered from Windows Update\Select when Preview Builds and Feature Updates are received
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **WindowsUpdate.admx/adml** that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Select when Feature Updates are received*, but it was renamed to *Select when Preview Builds and Feature Updates are received* starting with the Windows 10 Release 1709 Administrative Templates.

Default Value:

Disabled. (Feature Update cadence will not be enforced by Group Policy.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>7.3 Perform Automated Operating System Patch Management</u> Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v7	<u>2.4 Track Software Inventory Information</u> The software inventory system should track the name, version, publisher, and install date for all software, including operating systems authorized by the organization.			

18.10.92.4.3 Ensure 'Select when Quality Updates are received' is set to 'Enabled: 0 days' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This settings controls when Quality Updates are received.

The recommended state for this setting is: **Enabled: 0 days**.

Note: If the "Allow Diagnostic Data" (formerly "Allow Telemetry") policy is set to 0, this policy will have no effect.

Note #2: Starting with Windows Server 2016 RTM (Release 1607), Microsoft introduced a new Windows Update (WU) client behavior called **Dual Scan**, with an eye to cloud-based update management. In some cases, this Dual Scan feature can interfere with Windows Updates from Windows Server Update Services (WSUS) and/or manual WU updates. If you are using WSUS in your environment, you may need to set the above setting to **Not Configured** or configure the setting *Do not allow update deferral policies to cause scans against Windows Update* (added in the Windows 10 Release 1709 Administrative Templates) in order to prevent the Dual Scan feature from interfering. More information on Dual Scan is available at these links:

- [Demystifying "Dual Scan" – WSUS Product Team Blog](#)
- [Improving Dual Scan on 1607 – WSUS Product Team Blog](#)

Rationale:

Quality Updates can contain important bug fixes and/or security patches, and should be installed as soon as possible.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1** (DeferQualityUpdates) and **0** (DeferQualityUpdatesPeriodInDays).

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate:DeferQualityUpdates
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate:DeferQualityUpdatesPeriodInDays
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled:0 days**:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Update\Manage updates offered from Windows Update\Select
when Quality Updates are received
```

Note: This Group Policy path does not exist by default. An updated Group Policy template (**WindowsUpdate.admx/adml**) is required - it is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

Default Value:

Enabled: 0 days. (Install new Quality Updates as soon as they are available.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.3 <u>Perform Automated Operating System Patch Management</u> Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v7	3.4 <u>Deploy Automated Operating System Patch Management Tools</u> Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.			
v7	3.5 <u>Deploy Automated Software Patch Management Tools</u> Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.			

19 Administrative Templates (User)

This section contains user-based recommendations from Group Policy Administrative Templates (ADMX).

These settings are intended to harden the systems of users who log in interactively through a domain login, whether locally or via Remote Desktop Protocol (RDP). Group Policy and the associated registry keys in HKEY_USERS do not apply to non-interactive logins by design.

19.1 Control Panel

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.2 Desktop

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.3 Network

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.4 Shared Folders

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `SharedFolders.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.5 Start Menu and Taskbar

This section contains recommendations for Start Menu and Taskbar settings.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.5.1 Notifications

This section contains recommendations for Notification settings.

This Group Policy section is provided by the Group Policy template `WPN.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

19.5.1.1 Ensure 'Turn off toast notifications on the lock screen' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting turns off toast notifications on the lock screen.

The recommended state for this setting is **Enabled**.

Rationale:

While this feature can be handy for users, applications that provide toast notifications might display sensitive personal or business data while the device is left unattended.

Impact:

Applications will not be able to raise toast notifications on the lock screen.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKU\[USER  
SID]\Software\Policies\Microsoft\Windows\CurrentVersion\PushNotifications:NoT  
oastApplicationNotificationOnLockScreen
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
User Configuration\Policies\Administrative Templates\Start Menu and  
Taskbar\Notifications\Turn off toast notifications on the lock screen
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **WPN.admx/adml** that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (Toast notifications on the lock screen are enabled and can be turned off by the administrator or user.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>16.11 Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity.			

19.6 System

This section contains recommendations for System settings.

This Group Policy section is provided by the Group Policy template **Windows.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

19.6.1 Ctrl+Alt+Del Options

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template **CtrlAltDel.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

19.6.2 Display

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template **Display.admx/adml** that is included with the Microsoft Windows 10 Release 1803 Administrative Templates (or newer).

19.6.3 Driver Installation

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template **DeviceInstallation.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

19.6.4 Folder Redirection

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template **FolderRedirection.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

19.6.5 Group Policy

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `GroupPolicy.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.6.6 Internet Communication Management

This section contains recommendations related to Internet Communication Management.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.6.6.1 Internet Communication settings

This section contains recommendations related to Internet Communication settings.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.6.6.1.1 Ensure 'Turn off Help Experience Improvement Program' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting specifies whether users can participate in the Help Experience Improvement program. The Help Experience Improvement program collects information about how customers use Windows Help so that Microsoft can improve it.

The recommended state for this setting is: **Enabled**.

Rationale:

Large enterprise managed environments may not want to have information collected by Microsoft from managed client computers.

Impact:

Users cannot participate in the Help Experience Improvement program.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKU\[USER  
SID]\Software\Policies\Microsoft\Assistance\Client\1.0:NoImplicitFeedback
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
User Configuration\Policies\Administrative Templates\System\Internet  
Communication Management\Internet Communication Settings\Turn off Help  
Experience Improvement Program
```

Note: This Group Policy path is provided by the Group Policy template **HelpAndSupport.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Users can turn on the Help Experience Improvement program feature from the Help and Support settings page.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

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.

19.7.5.1 Ensure 'Do not preserve zone information in file attachments' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server
- STIG Domain Controller
- STIG Member Server

Description:

This policy setting allows you to manage whether Windows marks file attachments with information about their zone of origin (such as restricted, Internet, intranet, local). This requires NTFS in order to function correctly, and will fail without notice on FAT32. By not preserving the zone information, Windows cannot make proper risk assessments.

The recommended state for this setting is: **Disabled**.

Note: The Attachment Manager feature warns users when opening or executing files which are marked as being from an untrusted source, unless/until the file's zone information has been removed via the "Unblock" button on the file's properties or via a separate tool such as [Microsoft Sysinternals Streams](#).

Rationale:

A file that is downloaded from a computer in the Internet or Restricted Sites zone may be moved to a location that makes it appear safe, like an intranet file share, and executed by an unsuspecting user. The Attachment Manager feature will warn users when opening or executing files which are marked as being from an untrusted source, unless/until the file's zone information has been removed.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **2**.

```
HKU\[USER  
SID]\Software\Microsoft\Windows\CurrentVersion\Policies\Attachments:SaveZoneI  
nformation
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
User Configuration\Policies\Administrative Templates\Windows  
Components\Attachment Manager\Do not preserve zone information in file  
attachments
```

Note: This Group Policy path is provided by the Group Policy template **AttachmentManager.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Windows marks file attachments with their zone information.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225069
Rule ID: SV-225069r569186_rule
STIG ID: WN16-UC-000030
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

19.7.5.2 Ensure 'Notify antivirus programs when opening attachments' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting manages the behavior for notifying registered antivirus programs. If multiple programs are registered, they will all be notified.

The recommended state for this setting is: **Enabled**.

Note: An updated antivirus program must be installed for this policy setting to function properly.

Rationale:

Antivirus programs that do not perform on-access checks may not be able to scan downloaded files.

Impact:

Windows tells the registered antivirus program(s) to scan the file when a user opens a file attachment. If the antivirus program fails, the attachment is blocked from being opened.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **3**.

```
HKU\[USER  
SID]\Software\Microsoft\Windows\CurrentVersion\Policies\Attachments:ScanWithA  
ntiVirus
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
User Configuration\Policies\Administrative Templates\Windows  
Components\Attachment Manager\Notify antivirus programs when opening  
attachments
```

Note: This Group Policy path is provided by the Group Policy template **AttachmentManager.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Windows does not call the registered antivirus program(s) when file attachments are opened.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 <u>Deploy and Maintain Anti-Malware Software</u> Deploy and maintain anti-malware software on all enterprise assets.			
v7	8.1 <u>Utilize Centrally Managed Anti-malware Software</u> Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.			

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).

19.7.8.1 Ensure 'Configure Windows spotlight on lock screen' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting lets you configure Windows Spotlight on the lock screen.

The recommended state for this setting is: **Disabled**.

Note: [Per Microsoft TechNet](#), this policy setting only applies to Windows 10 Enterprise and Windows 10 Education editions.

Rationale:

Enabling this setting will help ensure your data is not shared with any third party. The Windows Spotlight feature collects data and uses that data to display suggested apps as well as images from the internet.

Impact:

Windows Spotlight will be turned off and users will no longer be able to select it as their lock screen.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **2**.

```
HKU\[USER  
SID]\Software\Policies\Microsoft\Windows\CloudContent:ConfigureWindowsSpotlight
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
User Configuration\Policies\Administrative Templates\Windows Components\Cloud  
Content\Configure Windows spotlight on lock screen
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **CloudContent.admx/adml** that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

Default Value:

Enabled. (Windows Spotlight is set as the lock screen provider.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	16.11 <u>Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

19.7.8.2 Ensure 'Do not suggest third-party content in Windows spotlight' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether Windows will suggest apps and content from third-party software publishers.

The recommended state for this setting is: **Enabled**.

Rationale:

Enabling this setting will help ensure your data is not shared with any third party. The Windows Spotlight feature collects data and uses that data to display suggested apps as well as images from the internet.

Impact:

Windows Spotlight on lock screen, Windows tips, Microsoft consumer features and other related features will no longer suggest apps and content from third-party software publishers. Users may still see suggestions and tips to make them more productive with Microsoft features and apps.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKU\[USER  
SID]\Software\Policies\Microsoft\Windows\CloudContent:DisableThirdPartySugge  
stions
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
User Configuration\Policies\Administrative Templates\Windows Components\Cloud  
Content\Do not suggest third-party content in Windows spotlight
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **CloudContent.admx/adml** that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

Default Value:

Disabled. (Apps and content from third-party software publishers will be suggested in addition to Microsoft apps and content.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

19.7.8.3 Ensure 'Do not use diagnostic data for tailored experiences' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This setting determines if Windows can use diagnostic data to provide tailored experiences to the user.

The recommended state for this setting is: **Enabled**.

Rationale:

Tracking, collection and utilization of personalized data is a privacy and security issue that is of concern to many organizations.

Impact:

Windows will not use diagnostic data from this device (this data may include browser, app and feature usage, depending on the "Diagnostic and usage data" setting value) to customize content shown on the lock screen, Windows tips, Microsoft consumer features and other related features. If these features are enabled, users will still see recommendations, tips and offers, but they may be less personalized.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKU\[USER  
SID]\Software\Policies\Microsoft\Windows\CloudContent:DisableTailoredExperiencesWithDiagnosticData
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
User Configuration\Policies\Administrative Templates\Windows Components\Cloud Content\Do not use diagnostic data for tailored experiences
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **CloudContent.admx/adml** that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

Default Value:

Disabled. (Microsoft will use diagnostic data to provide personalized recommendations, tips and offers.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

19.7.8.4 Ensure 'Turn off all Windows spotlight features' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting lets you turn off all Windows Spotlight features at once.

The recommended state for this setting is: **Enabled**.

Note: [Per Microsoft TechNet](#), this policy setting only applies to Windows 10 Enterprise and Windows 10 Education editions.

Rationale:

Enabling this setting will help ensure your data is not shared with any third party. The Windows Spotlight feature collects data and uses that data to display suggested apps as well as images from the internet.

Impact:

Windows Spotlight on lock screen, Windows tips, Microsoft consumer features and other related features will be turned off.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKU\[USER  
SID]\Software\Policies\Microsoft\Windows\CloudContent:DisableWindowsSpotlight  
Features
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
User Configuration\Policies\Administrative Templates\Windows Components\Cloud  
Content\Turn off all Windows spotlight features
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **CloudContent.admx/adml** that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

Default Value:

Disabled. (Windows Spotlight features are allowed.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

19.7.8.5 Ensure 'Turn off Spotlight collection on Desktop' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting removes the Spotlight collection setting in Personalization, rendering the user unable to select and subsequently download daily images from Microsoft to the system desktop.

The recommended state for this setting is: **Enabled**.

Rationale:

Enabling this setting will help ensure your data is not shared with any third party. The Windows Spotlight feature collects data and uses that data to display images from Microsoft.

Impact:

The **Spotlight collection** feature will not be available as an option in Personalization settings, so users will not be able to download daily images from Microsoft.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKU\[USER  
SID]\SOFTWARE\Policies\Microsoft\Windows\CloudContent:DisableSpotlightCollect  
ionOnDesktop
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
User Configuration\Policies\Administrative Templates\Windows Components\Cloud  
Content\Turn off Spotlight collection on Desktop
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **CloudContent.admx/adml** that is included with the Microsoft Windows 11 Release 21H2 Administrative Templates (or newer).

Default Value:

Disabled. (Spotlight collection will appear as an option in Personalization settings, allowing the user to select Spotlight collection as the Desktop provider and display daily images from Microsoft on the desktop.)

References:

1. <https://docs.microsoft.com/en-us/windows/configuration/windows-spotlight>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>0.0 Explicitly Not Mapped</u> Explicitly Not Mapped			

19.7.9 Credential User Interface

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template **CredUI.admx/adml** that is included with the Microsoft Windows 10 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 contains recommendations related to File Explorer.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note: This section was initially named *Windows Explorer* but was renamed by Microsoft to *File Explorer* starting with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

19.7.15.1 Explorer Frame Pane

This section contains recommendations related to Explorer Frame Pane.

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.

19.7.15.1.1 Ensure 'Turn off Preview Pane' is set to 'Enabled' (Automated)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting hides the Preview Pane in File Explorer.

The recommended STIG state for this setting is **Enabled**.

Rationale:

A known vulnerability in Windows could allow the execution of malicious code by either opening a compromised document or viewing it in the Windows Preview pane.

Impact:

Users will not be able to use or see the Preview Pane in File Explorer.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\[USER  
SID]\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer:NoReadingPan  
e
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
User Configuration\Policies\Administrative Templates\Windows Components\File  
Explorer\Explorer Frame Pane\Turn off Preview Pane
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **framepanes.admx/adml**.

Default Value:

Disabled. (The Preview Pane is hidden by default and can be displayed by the user.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-236000
Rule ID: SV-236000r641817_rule
STIG ID: WN16-CC-000421
Severity: CAT II

19.7.15.1.2 Ensure 'Turn on off details pane' is set to 'Enabled: Always hide' (Automated)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting shows or hides the Details Pane in File Explorer.

The recommended STIG state for this setting is **Enabled: Always hide**.

Rationale:

A known vulnerability in Windows could allow the execution of malicious code by either opening a compromised document or viewing it in the Windows Preview pane.

Impact:

Users will not be able to use or see the Details Pane in File Explorer.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\[USER  
SID]\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer:NoPreviewPan  
e
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled: Always hide**:

```
User Configuration\Policies\Administrative Templates\Windows Components\File  
Explorer\Explorer Frame Pane\Turn on off Details Pane
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template **framepanes.admx/adml**.

Default Value:

Disabled. (The Details Pane is hidden by default and can be displayed by the user.)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-236000
Rule ID: SV-236000r641817_rule
STIG ID: WN16-CC-000421
Severity: CAT II

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.

19.7.26.1 Ensure 'Prevent users from sharing files within their profile.' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether users can share files within their profile. By default, users are allowed to share files within their profile to other users on their network after an administrator opts in the computer. An administrator can opt in the computer by using the sharing wizard to share a file within their profile.

The recommended state for this setting is: **Enabled**.

Rationale:

If not properly configured, a user could accidentally share sensitive data with unauthorized users. In an enterprise managed environment, the company should provide a managed location for file sharing, such as a file server or SharePoint, instead of the user sharing files directly from their own user profile.

Impact:

Users cannot share files within their profile using the sharing wizard. Also, the sharing wizard cannot create a share at **%root%\Users** and can only be used to create SMB shares on folders.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKU\[USER  
SID]\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer:NoInplaceSha  
ring
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
User Configuration\Policies\Administrative Templates\Windows  
Components\Network Sharing\Prevent users from sharing files within their  
profile.
```

Note: This Group Policy path is provided by the Group Policy template **Sharing.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Users can share files out of their user profile after an administrator has opted in the computer.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	14.6 <u>Protect Information through Access Control Lists</u> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

19.7.27 OOB

This section is 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 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.

19.7.33 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).

19.7.34 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.

19.7.35 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.

19.7.36 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.

19.7.37 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.

19.7.38 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).

19.7.39 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).

19.7.40 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.

19.7.41 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.

19.7.42 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.

19.7.42.1 Ensure 'Always install with elevated privileges' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This setting controls whether or not Windows Installer should use system permissions when it installs any program on the system.

Note: This setting appears both in the Computer Configuration and User Configuration folders. To make this setting effective, you must enable the setting in both folders.

Caution: If enabled, skilled users can take advantage of the permissions this setting grants to change their privileges and gain permanent access to restricted files and folders. Note that the User Configuration version of this setting is not guaranteed to be secure.

The recommended state for this setting is: **Disabled**.

Rationale:

Users with limited privileges can exploit this feature by creating a Windows Installer installation package that creates a new local account that belongs to the local built-in Administrators group, adds their current account to the local built-in Administrators group, installs malicious software, or performs other unauthorized activities.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **0**.

```
HKU\[USER  
SID]\Software\Policies\Microsoft\Windows\Installer:AlwaysInstallElevated
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Disabled**:

```
User Configuration\Policies\Administrative Templates\Windows  
Components\Windows Installer\Always install with elevated privileges
```

Note: This Group Policy path is provided by the Group Policy template **MSI.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Windows Installer will apply the current user's permissions when it installs programs that a system administrator does not distribute or offer. This will prevent standard users from installing applications that affect system-wide configuration items.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	4.3 <u>Ensure the Use of Dedicated Administrative Accounts</u> Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●

19.7.43 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.

19.7.44 Windows Media Player

This section contains recommendations related to Windows Media Player.

This Group Policy section is provided by the Group Policy template [WindowsMediaPlayer.admx/adml](#) that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.44.1 Networking

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template [WindowsMediaPlayer.admx/adml](#) that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.44.2 Playback

This section contains recommendations related to Windows Media Player playback.

This Group Policy section is provided by the Group Policy template [WindowsMediaPlayer.admx/adml](#) that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.44.2.1 Ensure 'Prevent Codec Download' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This setting controls whether Windows Media Player is allowed to download additional codecs for decoding media files it does not already understand.

The recommended state for this setting is: **Enabled**.

Rationale:

This has some potential for risk if a malicious data file is opened in Media Player that requires an additional codec to be installed. If a special codec is required for a necessary job function, then that codec should first be tested to ensure it is legitimate, and it should be supplied by the IT department in the organization.

Impact:

Windows Media Player is prevented from automatically downloading codecs to your computer. In addition, the *Download codecs automatically* check box on the Player tab in the Player is not available.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a **REG_DWORD** value of **1**.

```
HKU\[USER  
SID]\Software\Policies\Microsoft\WindowsMediaPlayer:PreventCodecDownload
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:

```
User Configuration\Policies\Administrative Templates\Windows  
Components\Windows Media Player\Playback\Prevent Codec Download
```

Note: This Group Policy path is provided by the Group Policy template **WindowsMediaPlayer.admx/adml** that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Users can change the setting for the *Download codecs automatically* check box.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

20 Additional Security Technical Implementation Guide (STIG) Settings

This section contains additional Security Technical Implementation Guide (STIG) settings that may not be controlled through Group Policy.

20.1 Ensure 'Accounts require passwords' (Manual)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting ensures that all accounts are password protected.

Rationale:

The lack of password protection enables anyone to gain access to the system, which opens a backdoor opportunity for intruders to compromise the system as well as other resources.

Impact:

All accounts will be required to have a password for protection.

Audit:

Verify that all accounts have passwords:

Domain Controllers

- In PowerShell run the following command:

```
Get-Aduser -Filter * -Properties Passwordnotrequired | FT Name, Passwordnotrequired, Enabled
```

- Ensure that no entries for **Passwordnotrequired** is marked **True** or **blank** for any enabled user account.

Note: Exclude disabled accounts (e.g., DefaultAccount, Guest) and Trusted Domain Objects (TDOs).

Member servers and standalone systems

- In PowerShell run the following command:

```
Get-CimInstance -Class Win32_Useraccount -Filter "PasswordRequired=False and LocalAccount=True" | FT Name, PasswordRequired, Disabled, LocalAccount
```

- Ensure that no entries for **Passwordnotrequired** are marked **False**.

Note: Exclude disabled accounts (e.g., DefaultAccount, Guest).

Remediation:

Configure all enabled accounts to require passwords.

Note: The password required flag can be set by entering the following on a command line:

```
Net user [username] /passwordreq:yes
```

Substitute [username] with the name of the user account.

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224838
Rule ID: SV-224838r857232_rule
STIG ID: WN16-00-000220
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 <u>Use Unique Passwords</u> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v7	4.4 <u>Use Unique Passwords</u> Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			

20.2 Ensure 'Active Directory AdminSDHolder object is configured with proper audit settings' (STIG DC only) (Manual)

Profile Applicability:

- STIG Domain Controller

Description:

This policy setting ensures that the Active Directory **AdminSDHolder** object is configured with the proper audit settings.

The recommended STIG state for this setting is: **Type - Fail, Principal - Everyone, Access - Full Control, Inherited from - None, and Applies to - This object only**

Rationale:

When inappropriate audit settings are configured for directory service database objects, it may be possible for a user or process to update the data without generating any tracking data.

The impact of missing audit data is related to the type of object. A failure to capture audit data for objects used by identification, authentication, or authorization functions could degrade or eliminate the ability to track changes to access policy for systems or data.

For Active Directory (AD), there are a number of critical object types in the domain naming context of the AD database for which auditing is essential. This includes the **AdminSDHolder** object. Because changes to these objects can significantly impact access controls or the availability of systems, the absence of auditing data makes it impossible to identify the source of changes that impact the confidentiality, integrity, and availability of data and systems throughout an AD domain. The lack of proper auditing can result in insufficient forensic evidence needed to investigate an incident and prosecute the intruder.

Impact:

None - this is the default behavior.

Audit:

Verify that the *AdminSDHolder* object is configured with at least the following permissions: **Type - Fail**, **Principal - Everyone**, **Access - Full Control**, **Inherited from - None**, and **Applies to - This object only**

- Open *Active Directory Users and Computers*
- Ensure *Advanced Features* is selected in the *View* menu
- Select *System* under the domain being reviewed
- Right-click the *AdminSDHolder* object
- Select *Properties*
- Select the *Security* tab
- Select the *Advanced* button
- Select the *Auditing* tab.

Ensure the above auditing permissions are set.

Remediation:

Configure the audit settings for *AdminSDHolder* object to include at least the following:

Type - Fail, Principal - Everyone, Access - Full Control, Inherited from - None, and Applies to - This object only

- Open *Active Directory Users and Computers*
- Ensure *Advanced Features* is selected in the *View* menu
- Select *System* under the domain being reviewed
- Right-click the *AdminSDHolder* object
- Select *Properties*
- Select the *Security* tab
- Select the *Advanced* button
- Select the *Auditing* tab.

Configure the above audit permission settings.

Note: The success types listed below are defaults. Where Special is listed in the summary screens for Access, detailed Permissions are provided for reference. Various Properties selections may also exist by default.

- Type - Success
- Principal - Everyone
- Access - Special
- Inherited from - None
- Applies to - This object only
- (Access - Special = Write all properties, Modify permissions, Modify owner)

Two instances with the following summary information will be listed:

- Type - Success
- Principal - Everyone
- Access - (blank)
- Inherited from - (CN of domain)
- Applies to - Descendant Organizational Unit objects

Default Value:

Type - Success; Principal - Everyone; Access - Special; Inherited from - None; Applies to - This object only

(Access - Special = Write all properties, Modify permissions, Modify owner)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224984
Rule ID: SV-224984r852356_rule
STIG ID: WN16-DC-000210
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

20.3 Ensure 'Active Directory Domain Controllers Organizational Unit (OU) object have the proper access control permissions' (STIG DC only) (Manual)

Profile Applicability:

- STIG Domain Controller

Description:

This policy setting ensures that Active Directory Domain Controllers Organizational Unit (OU) objects have the proper access control permissions.

The recommended STIG state for this setting is: **System, Domain Admins, Enterprise Admins, and Administrators**

Rationale:

When Active Directory objects do not have appropriate access control permissions, it may be possible for malicious users to create, read, update, or delete the objects and degrade or destroy the integrity of the data. When the directory service is used for identification, authentication, or authorization functions, a compromise of the database objects could lead to a compromise of all systems that rely on the directory service.

The Domain Controllers OU object requires special attention as the Domain Controllers are central to the configuration and management of the domain. Inappropriate access permissions defined for the Domain Controllers OU could allow intruders or unauthorized personnel to make changes that could lead to the compromise of the domain.

Impact:

Only authorized users will have access control permissions.

Audit:

Verify access control permissions on the Domain Controllers OU are: **System, Domain Admins, Enterprise Admins** and **Administrators**

- Open *Active Directory Users and Computers*
- Ensure *Advanced Features* is selected in the *View* menu
- Select the *Domain Controllers* OU
- Right-click and select *Properties*
- Select the *Security* tab

Note The default permissions listed below satisfy this requirement. The permissions shown are at the summary level. More detailed permissions can be viewed by selecting the *Advanced* button, the desired Permission entry, and the *View* or *Edit* button.

Note #2 Except where noted otherwise, the special permissions may include a wide range of permissions and properties and are acceptable for this requirement.

Summary:

CREATOR OWNER - Special permissions, **SELF** - Special permissions, and **Authenticated Users** - Read, Special permissions

Detailed:

SYSTEM - Full Control, **Domain Admins** - Read, Write, Create all child objects, Generate resultant set of policy (logging), Generate resultant set of policy (planning), Special permissions, **Enterprise Admins** - Full Control, **Key Admins** - Special permissions, **Enterprise Key Admins** - Special permissions, **Administrators** - Read, Write, Create all child objects, Generate resultant set of policy (logging), and Generate resultant set of policy (planning), Special permissions, **Pre-Windows 2000 Compatible Access** - Special permissions, and **ENTERPRISE DOMAIN CONTROLLERS** - Read, Special permissions

Note: Domains supporting Microsoft Exchange will have additional Exchange related permissions on the Domain Controllers OU. These may include some change related permissions and are not a finding.

Note #2: The Special permissions for Pre-Windows 2000 Compatible Access are Read types.

Note #3: If detailed permissions include any Create, Delete, Modify, or Write Permissions or Properties it is not in compliance with this recommendation.

Note #4: The special permissions for Authenticated Users are Read types. If detailed permissions include any Create, Delete, Modify, or Write Permissions or Properties it is not in compliance with this recommendation.

Remediation:

Limit the permissions on the Domain Controllers OU to restrict changes to: **System**, **Domain Admins**, **Enterprise Admins** and **Administrators**.

- Open *Active Directory Users and Computers*
- Ensure *Advanced Features* is selected in the *View* menu
- Select the *Domain Controllers* OU
- Right-click and select *Properties*
- Select the *Security* tab

Ensure the permissions are set to the above recommendation.

Note The default permissions listed below satisfy this requirement. The permissions shown are at the summary level. More detailed permissions can be viewed by selecting the *Advanced* button, the desired Permission entry, and the *View* or *Edit* button.

Note #2 Except where noted otherwise, the special permissions may include a wide range of permissions and properties and are acceptable for this requirement.

Summary:

CREATOR OWNER - Special permissions, **SELF** - Special permissions, and **Authenticated Users** - Read, Special permissions

The special permissions for Authenticated Users are Read types. If detailed permissions include any Create, Delete, Modify, or Write Permissions or Properties it is not in compliance with this recommendation.

Detailed:

SYSTEM - Full Control, **Domain Admins** - Read, Write, Create all child objects, Generate resultant set of policy (logging), Generate resultant set of policy (planning), Special permissions, **Enterprise Admins** - Full Control, **Key Admins** - Special permissions, **Enterprise Key Admins** - Special permissions, **Administrators** - Read, Write, Create all child objects, Generate resultant set of policy (logging), and Generate resultant set of policy (planning), Special permissions, **Pre-Windows 2000 Compatible Access** - Special permissions, and **ENTERPRISE DOMAIN CONTROLLERS** - Read, Special permissions

Note: The Special permissions for Pre-Windows 2000 Compatible Access are Read types.

Note #2: If detailed permissions include any Create, Delete, Modify, or Write Permissions or Properties it is not in compliance with this recommendation.

Default Value:

SYSTEM - Full Control, Domain Admins - Read, Write, Create all child objects, Generate resultant set of policy (logging), Generate resultant set of policy (planning), Special permissions, Enterprise Admins - Full Control, Key Admins - Special permissions, Enterprise Key Admins - Special permissions, Administrators - Read, Write, Create all child objects, Generate resultant set of policy (logging), and Generate resultant set of policy (planning), Special permissions, Pre-Windows 2000 Compatible Access - Special permissions, and ENTERPRISE DOMAIN CONTROLLERS - Read, Special permissions

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224973
Rule ID: SV-224973r877392_rule
STIG ID: WN16-DC-000100
Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

20.4 Ensure 'Active Directory Domain Controllers Organizational Unit (OU) object is configured with proper audit settings' (STIG DC only) (Manual)

Profile Applicability:

- STIG Domain Controller

Description:

This policy setting ensures that the Active Directory Domain Controllers Organizational Unit (OU) object is configured with the proper audit settings.

The recommended STIG state for this setting is: **Type - Fail, Principal - Everyone, Access - Full Control, and Inherited from - None.**

Note: These audit settings apply to this object and all descendant objects.

Rationale:

When inappropriate audit settings are configured for directory service database objects, it may be possible for a user or process to update the data without generating any tracking data.

The impact of missing audit data is related to the type of object. A failure to capture audit data for objects used by identification, authentication, or authorization functions could degrade or eliminate the ability to track changes to access policy for systems or data.

For Active Directory (AD), there are a number of critical object types in the domain naming context of the AD database for which auditing is essential. This includes the Domain Controllers Organizational Unit (OU) object. Because changes to these objects can significantly impact access controls or the availability of systems, the absence of auditing data makes it impossible to identify the source of changes that impact the confidentiality, integrity, and availability of data and systems throughout an AD domain. The lack of proper auditing can result in insufficient forensic evidence needed to investigate an incident and prosecute the intruder.

Impact:

None - this is the default behavior.

Audit:

Verify that the *Domain Controllers Organizational Unit (OU)* object is configured with at least the following: **Type - Fail**, **Principal - Everyone**, **Access - Full Control**, and **Inherited from - None**. These audit settings apply to this object and all descendant objects.

- Open *Active Directory Users and Computers*
- Ensure *Advanced Features* is selected in the *View* menu
- Select *System* under the domain being reviewed
- Right-click the *Domain Controllers Organizational Unit (OU)* object and select *Properties*
- Select the *Security* tab
- Select the *Advanced* button
- Select the *Auditing* tab

Ensure the above auditing permissions are set.

Remediation:

Configure the audit settings for *Domain Controllers Organizational Unit (OU)* object to include at least the following: **Type - Fail**, **Principal - Everyone**, **Access - Full Control**, and **Inherited from - None**.

- Open *Active Directory Users and Computers*
- Ensure *Advanced Features* is selected in the *View* menu
- Select *System* under the domain being reviewed
- Right-click the *Domain Controllers Organizational Unit (OU)* object and select *Properties*
- Select the *Security* tab
- Select the *Advanced* button
- Select the *Auditing* tab

Note: These audit settings apply to this object and all descendant objects.

Note #2: The success types listed below are defaults. Where Special is listed in the summary screens for Access, detailed Permissions are provided for reference. Various Properties selections may also exist by default.

- Type - Success
- Principal - Everyone
- Access - Special
- Inherited from - None
- (Access - Special = Write all properties, All extended rights, Change RID master)

Two instances with the following summary information will be listed:

- Type - Success
- Principal - Everyone
- Access - (blank)
- Inherited from - (CN of domain)

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224983
Rule ID: SV-224983r852355_rule
STIG ID: WN16-DC-000200
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

20.5 Ensure 'Active Directory Domain object is configured with proper audit settings' (STIG DC only) (Manual)

Profile Applicability:

- STIG Domain Controller

Description:

This policy setting ensures that the Active Directory Domain object is configured with the proper audit settings.

The recommended STIG state for this setting is: **Type - Fail, Principal - Everyone, Access - Full Control**, and **Inherited from - None**. These audit settings apply to this object only.

Rationale:

When inappropriate audit settings are configured for directory service database objects, it may be possible for a user or process to update the data without generating any tracking data.

The impact of missing audit data is related to the type of object. A failure to capture audit data for objects used by identification, authentication, or authorization functions could degrade or eliminate the ability to track changes to access policy for systems or data.

For Active Directory (AD), there are a number of critical object types in the domain naming context of the AD database for which auditing is essential. This includes the Domain object. Because changes to these objects can significantly impact access controls or the availability of systems, the absence of auditing data makes it impossible to identify the source of changes that impact the confidentiality, integrity, and availability of data and systems throughout an AD domain. The lack of proper auditing can result in insufficient forensic evidence needed to investigate an incident and prosecute the intruder.

Impact:

None - this is the default behavior.

Audit:

Verify that the *Domain* object is configured with at least the following: **Type - Fail**, **Principal - Everyone**, **Access - Full Control**, and **Inherited from - None**. These audit settings apply to this object only.

- Open *Active Directory Users and Computers*
- Ensure *Advanced Features* is selected in the *View* menu
- Select *System* under the domain being reviewed
- Right-click the *Domain* object and select *Properties*
- Select the *Security* tab
- Select the *Advanced* button
- Select the *Auditing* tab

Ensure the above auditing permissions are set.

Remediation:

Configure audit settings for *Domain* object to include at least the following: **Type - Fail**, **Principal - Everyone**, **Access - Full Control**, and **Inherited from - None**. These audit settings apply to this object only.

- Open *Active Directory Users and Computers*
- Ensure *Advanced Features* is selected in the *View* menu
- Select *System* under the domain being reviewed
- Right-click the *Domain* object and select *Properties*
- Select the *Security* tab
- Select the *Advanced* button
- Select the *Auditing* tab

Note: The success types listed below are defaults. Where Special is listed in the summary screens for Access, detailed Permissions are provided for reference. Various Properties selections may also exist by default.

Two instances with the following summary information will be listed:

- Type - Success
- Principal - Everyone
- Access - (blank)
- Inherited from - None
- Applies to - Special

OR

- Type - Success
- Principal - Domain Users
- Access - All extended rights
- Inherited from - None

Applies to - This object only

- Type - Success
- Principal - Administrators
- Access - All extended rights
- Inherited from - None

Applies to - This object only

OR

- Type - Success
- Principal - Everyone
- Access - Special
- Inherited from - None

Applies to - This object only

(Access - Special = Permissions: Write all properties, Modify permissions, Modify owner)

Default Value:

Type - Success; Principal - Everyone; Access - (blank); Inherited from - None; Applies to – Special

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224981
Rule ID: SV-224981r852353_rule
STIG ID: WN16-DC-000180
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

20.6 Ensure 'Active Directory Group Policy objects are configured with proper audit settings' (STIG DC only) (Manual)

Profile Applicability:

- STIG Domain Controller

Description:

This policy setting ensures that the Active Directory Group Policy objects are configured with the proper audit settings.

The recommended STIG state for this setting is: **Type - Fail, Principal - Everyone, and Access - Full Control.**

Note: These audit settings apply to this object and all descendant objects or Descendant **groupPolicyContainer** objects.

Rationale:

When inappropriate audit settings are configured for directory service database objects, it may be possible for a user or process to update the data without generating any tracking data.

The impact of missing audit data is related to the type of object. A failure to capture audit data for objects used by identification, authentication, or authorization functions could degrade or eliminate the ability to track changes to access policy for systems or data.

For Active Directory (AD), there are a number of critical object types in the domain naming context of the AD database for which auditing is essential. This includes the Group Policy objects. Because changes to these objects can significantly impact access controls or the availability of systems, the absence of auditing data makes it impossible to identify the source of changes that impact the confidentiality, integrity, and availability of data and systems throughout an AD domain. The lack of proper auditing can result in insufficient forensic evidence needed to investigate an incident and prosecute the intruder.

Impact:

None - this is the default behavior.

Audit:

Verify that *Group Policy* objects are configured with at least the following: **Type - Fail**, **Principal - Everyone**, **Access - Full Control**, and **Inherited from - None**.

- Open *Group Policy Management*
- Navigate to *Group Policy Objects* in the domain being reviewed (Forest > Domains > Domain).

For each Group Policy object:

- Select the *Group Policy object* item in the left pane
- Select the *Delegation* tab in the right pane
- Select the *Advanced* button
- Select the *Advanced* button again
- Select the *Auditing* tab

Ensure at least the above auditing permissions are set.

Note: These audit settings apply to this object and all descendant objects or Descendant groupPolicyContainer objects.

Remediation:

Configure the audit settings for *Group Policy* objects to include at least the following: **Type - Fail**, **Principal - Everyone**, **Access - Full Control**, and **Inherited from - None**.

Note: These audit settings apply to this object and all descendant objects or Descendant groupPolicyContainer objects.

- Open *Active Directory Users and Computers*
- Ensure *Advanced Features* is selected in the *View* menu
- Select *System* under the domain being reviewed
- Right-click *Policies* and select *Properties*
- Select the *Security* tab
- Select the *Advanced* button
- Select the *Auditing* tab

Ensure at least the above auditing permissions are set.

Note: The three Success types listed below are defaults inherited from the Parent Object. Where Special is listed in the summary screens for Access, detailed Permissions are provided for reference.

- Type - Success
- Principal - Everyone
- Access - Special (Permissions: Write all properties, Modify permissions; Properties: all "Write" type selected)
- Inherited from - Parent Object

Applies to - Descendant groupPolicyContainer objects

Two instances with the following summary information will be listed:

- Type - Success
- Principal - Everyone
- Access - blank (Permissions: none selected; Properties: one instance - Write gPLink, one instance - Write gPOptions)
- Inherited from - Parent Object

Applies to - Descendant Organization Unit Objects

Default Value:

Type - Success; Principal - Everyone; Access - Special (Permissions: Write all properties, Modify permissions; Properties: all "Write" type selected); Inherited from - Parent Object; Applies to - Descendant groupPolicyContainer objects

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224980
Rule ID: SV-224980r852352_rule
STIG ID: WN16-DC-000170
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

20.7 Ensure 'Active Directory Group Policy objects have proper access control permissions' (STIG DC only) (Manual)

Profile Applicability:

- STIG Domain Controller

Description:

This policy setting ensures that Active Directory Group Policy objects have proper access control permissions.

Rationale:

When directory service database objects do not have appropriate access control permissions, it may be possible for malicious users to create, read, update, or delete the objects and degrade or destroy the integrity of the data. When the directory service is used for identification, authentication, or authorization functions, a compromise of the database objects could lead to a compromise of all systems relying on the directory service.

For Active Directory (AD), the Group Policy objects require special attention. In a distributed administration model (i.e., help desk), Group Policy objects are more likely to have access permissions changed from the secure defaults. If inappropriate access permissions are defined for Group Policy objects, this could allow an intruder to change the security policy applied to all domain client computers (workstations and servers).

Impact:

Only authorized users will have access control permissions.

Audit:

Verify permissions on Group Policy objects via the *Group Policy Management Console*:

- Open *Group Policy Management Console*
- Navigate to the *Group Policy Objects* in the domain being reviewed.

For each Group Policy object:

- Select the *Group Policy object* item in the left pane
- Select the *Delegation* tab in the right pane
- Select the *Advanced* button
- Select each Group or user name

Review the permissions. If any standard user accounts or groups have "Allow" permissions greater than *Read* and *Apply group policy* it is not in compliance with this recommendation.

Other access permissions that allow the objects to be updated are considered not in compliance unless specifically documented by the ISSO.

The default permissions noted below satisfy this requirement.

The permissions shown are at the summary level. More detailed permissions can be viewed by selecting the next "Advanced" button, the desired Permission entry, and the "Edit" button.

Authenticated Users - Read, Apply group policy, Special permissions

The special permissions for Authenticated Users are for Read-type Properties. If detailed permissions include any Create, Delete, Modify, or Write Permissions or Properties, this is not in compliance.

The special permissions for the following default groups are not the focus of this requirement and may include a wide range of permissions and properties:

CREATOR OWNER - Special permissions, SYSTEM - Read, Write, Create all child objects, Delete all child objects, Special permissions, Domain Admins - Read, Write, Create all child objects, Delete all child objects, Special permissions, Enterprise Admins - Read, Write, Create all child objects, Delete all child objects, Special permissions, and ENTERPRISE DOMAIN CONTROLLERS - Read, Special permissions

The Domain Admins and Enterprise Admins will not have the *Delete all child objects* permission on the two default Group Policy objects: Default Domain Policy and Default Domain Controllers Policy. They will have this permission on organization created Group Policy objects.

Remediation:

Maintain the permissions on Group Policy objects to not allow greater than *Read* and *Apply group policy* for standard user accounts or groups.

The default permissions below meet this requirement:

Authenticated Users - Read, Apply group policy, Special permissions

The special permissions for Authenticated Users are for Read-type Properties.

CREATOR OWNER - Special permissions, SYSTEM - Read, Write, Create all child objects, Delete all child objects, Special permissions, Domain Admins - Read, Write, Create all child objects, Delete all child objects, Special permissions, Enterprise Admins - Read, Write, Create all child objects, Delete all child objects, Special permissions, and ENTERPRISE DOMAIN CONTROLLERS - Read, Special permissions

Document any other access permissions that allow the objects to be updated with the ISSO.

The Domain Admins and Enterprise Admins will not have the *Delete all child objects* permission on the two default Group Policy objects: Default Domain Policy and Default Domain Controllers Policy. They will have permission on created Group Policy objects.

Default Value:

Authenticated Users - Read, Apply group policy, Special permissions, CREATOR OWNER - Special permissions, SYSTEM - Read, Write, Create all child objects, Delete all child objects, Special permissions, Domain Admins - Read, Write, Create all child objects, Delete all child objects, Special permissions, Enterprise Admins - Read, Write, Create all child objects, Delete all child objects, Special permissions, and ENTERPRISE DOMAIN CONTROLLERS - Read, Special permissions

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224972
Rule ID: SV-224972r877392_rule
STIG ID: WN16-DC-000090
Severity: CAT I

20.8 Ensure 'Active Directory Infrastructure object is configured with proper audit settings' (STIG DC only) (Manual)

Profile Applicability:

- STIG Domain Controller

Description:

This policy setting ensures that the Active Directory Infrastructure object is configured with the proper audit settings.

The recommended STIG state for this setting is: **Type - Fail, Principal - Everyone, Access - Full Control, and Inherited from - None.**

Rationale:

When inappropriate audit settings are configured for directory service database objects, it may be possible for a user or process to update the data without generating any tracking data.

The impact of missing audit data is related to the type of object. A failure to capture audit data for objects used by identification, authentication, or authorization functions could degrade or eliminate the ability to track changes to access policy for systems or data.

For Active Directory (AD), there are a number of critical object types in the domain naming context of the AD database for which auditing is essential. This includes the Infrastructure object. Because changes to these objects can significantly impact access controls or the availability of systems, the absence of auditing data makes it impossible to identify the source of changes that impact the confidentiality, integrity, and availability of data and systems throughout an AD domain. The lack of proper auditing can result in insufficient forensic evidence needed to investigate an incident and prosecute the intruder.

Impact:

None - this is the default behavior.

Audit:

Verify that the *Infrastructure* object is configured with at least the following permissions:

Type - Fail, Principal - Everyone, Access - Full Control, and Inherited from - None.

- Open *Active Directory Users and Computers*
- Ensure *Advanced Features* is selected in the *View* menu
- Select *System* under the domain being reviewed
- Right-click the *Infrastructure* object and select *Properties*
- Select the *Security* tab
- Select the *Advanced* button
- Select the *Auditing* tab

Ensure the above auditing permissions are set.

Remediation:

Configure the audit settings for *Infrastructure* object to include at least the following:
Type - Fail, Principal - Everyone, Access - Full Control, and Inherited from - None.

- Open *Active Directory Users and Computers*
- Ensure *Advanced Features* is selected in the *View* menu
- Select *System* under the domain being reviewed
- Right-click the *Infrastructure* object and select *Properties*
- Select the *Security* tab
- Select the *Advanced* button
- Select the *Auditing* tab

Configure the above audit permission settings.

Note: The success types listed below are defaults. Where Special is listed in the summary screens for Access, detailed Permissions are provided for reference. Various Properties selections may also exist by default.

- Type - Success
- Principal - Everyone
- Access - Special
- Inherited from - None
- (Access - Special = Write all properties, All extended rights, Change RID master)

Two instances with the following summary information will be listed:

- Type - Success
- Principal - Everyone
- Access - (blank)
- Inherited from - (CN of domain)

Default Value:

Type - Success; Principal - Everyone; Access - Special; Inherited from - None; (Access - Special = Write all properties, All extended rights, Change RID master)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224982
Rule ID: SV-224982r852354_rule
STIG ID: WN16-DC-000190
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

20.9 Ensure 'Active Directory RID Manager\$ object is configured with proper audit settings' (STIG DC only) (Manual)

Profile Applicability:

- STIG Domain Controller

Description:

This policy setting ensures that the Active Directory RID Manager\$ object is configured with the proper audit settings.

The recommended STIG state for this setting is: **Type - Fail, Principal - Everyone, Access - Full Control, and Inherited from - None**

Rationale:

When inappropriate audit settings are configured for directory service database objects, it may be possible for a user or process to update the data without generating any tracking data.

The impact of missing audit data is related to the type of object. A failure to capture audit data for objects used by identification, authentication, or authorization functions could degrade or eliminate the ability to track changes to access policy for systems or data.

For Active Directory (AD), there are a number of critical object types in the domain naming context of the AD database for which auditing is essential. This includes the RID Manager\$ object. Because changes to these objects can significantly impact access controls or the availability of systems, the absence of auditing data makes it impossible to identify the source of changes that impact the confidentiality, integrity, and availability of data and systems throughout an AD domain. The lack of proper auditing can result in insufficient forensic evidence needed to investigate an incident and prosecute the intruder.

Impact:

None - this is the default behavior.

Audit:

Verify that the *RID Manager\$* object is configured with at least the following permissions: **Type - Fail**, **Principal - Everyone**, **Access - Full Control**, and **Inherited from - None**

- Open *Active Directory Users and Computers*
- Ensure *Advanced Features* is selected in the *View* menu
- Select *System* under the domain being reviewed
- Right-click the *RID Manager\$* object and select *Properties*
- Select the *Security* tab
- Select the *Advanced* button
- Select the *Auditing* tab

Ensure the above auditing permissions are set.

Remediation:

Configure the audit settings for *RID Manager\$* object to include at least the following:
Type - Fail, Principal - Everyone, Access - Full Control, and Inherited from - None

- Open *Active Directory Users and Computers*
- Ensure *Advanced Features* is selected in the *View* menu
- Select *System* under the domain being reviewed
- Right-click the *RID Manager\$* object and select *Properties*
- Select the *Security* tab
- Select the *Advanced* button
- Select the *Auditing* tab

Configure the above audit permissions.

Note: The success types listed below are defaults. Where Special is listed in the summary screens for Access, detailed Permissions are provided for reference. Various Properties selections may also exist by default.

- Type - Success
- Principal - Everyone
- Access - Special
- Inherited from - None
- (Access - Special = Write all properties, All extended rights, Change RID master)

Two instances with the following summary information will be listed:

- Type - Success
- Principal - Everyone
- Access - (blank)
- Inherited from - (CN of domain)

Default Value:

Type - Success; Principal - Everyone; Access - Special; Inherited from - None; (Access - Special = Write all properties, All extended rights, Change RID master)

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224985
Rule ID: SV-224985r852357_rule
STIG ID: WN16-DC-000220
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

20.10 Ensure 'Active Directory SYSVOL directory must have the proper access control permissions' (STIG DC only) (Manual)

Profile Applicability:

- STIG Domain Controller

Description:

This policy setting ensures that the Active Directory SYSVOL directory has proper access control permissions.

The recommended STIG state for this setting is: NT AUTHORITY\Authenticated Users:(RX), NT AUTHORITY\Authenticated Users:(OI)(CI)(IO)(GR,GE), BUILTIN\Server Operators:(RX), BUILTIN\Server Operators:(OI)(CI)(IO)(GR,GE), BUILTIN\Administrators:(M,WDAC,W0), BUILTIN\Administrators:(OI)(CI)(IO)(F), NT AUTHORITY\SYSTEM:(F), NT AUTHORITY\SYSTEM:(OI)(CI)(IO)(F), and CREATOR OWNER:(OI)(CI)(IO)(F)

Rationale:

Improper access permissions for directory data files could allow unauthorized users to read, modify, or delete directory data.

Impact:

Users that do not have access will not be able to read, modify, or delete directory data or audit trails.

Audit:

Verify that the following permissions are present for SYSVOL:

- Open the *Command Prompt*
- Type *icacls c:\Windows\SYSVOL*

The following results should be displayed:

NT AUTHORITY\Authenticated Users:(RX), NT AUTHORITY\Authenticated Users:(OI)(CI)(IO)(GR,GE), BUILTIN\Server Operators:(RX), BUILTIN\Server Operators:(OI)(CI)(IO)(GR,GE), BUILTIN\Administrators:(M,WDAC,W0), BUILTIN\Administrators:(OI)(CI)(IO)(F), NT AUTHORITY\SYSTEM:(F), NT AUTHORITY\SYSTEM:(OI)(CI)(IO)(F), and CREATOR OWNER:(OI)(CI)(IO)(F)

(RX) = Read & execute

Run *icacls /help* to view definitions of other permission codes.
Alternately check you can view permission via *File Explorer*.

- Open *File Explorer*
- Navigate to *\Windows\SYSVOL* (or the directory noted previously if different)
- Right-click the directory and select *properties*
- Select the *Security* tab
- Click *Advanced*

Permissions should be the following:

C:\Windows\SYSVOL

Type - "Allow" for all

Inherited from - "None" for all

Principal - Access - Applies to

Authenticated Users - Read & execute - This folder, subfolder, and files, Server Operators - Read & execute- This folder, subfolder, and files, Administrators - Special - This folder only (Special = Basic Permissions: all selected except Full control), CREATOR OWNER - Full control - Subfolders and files only, Administrators - Full control - Subfolders and files only, and SYSTEM - Full control - This folder, subfolders, and files

Remediation:

Modify permissions on the SYSVOL directory, if necessary. Do not allow greater than **Read & execute** permissions for standard user accounts or groups. The defaults below meet this requirement:

- Open *File Explorer*
- Navigate to *\Windows\SYSVOL* (or the directory noted previously if different)
- Right-click the directory and select *properties*
- Select the *Security* tab
- Click *Advanced*

Configure the audit permission settings.

C:\Windows\SYSVOL

Type - "Allow" for all

Inherited from - "None" for all

Principal - Access - Applies to

Authenticated Users - Read & execute - This folder, subfolder, and files, Server Operators - Read & execute- This folder, subfolder, and files, Administrators - Special - This folder only (Special = Basic Permissions: all selected except Full control), CREATOR OWNER - Full control - Subfolders and files only, Administrators - Full control - Subfolders and files only, and SYSTEM - Full control - This folder, subfolders, and files

Default Value:

C:\Windows\SYSVOL Type - "Allow" for all Inherited from - "None" for all

Principal - Access - Applies to

Authenticated Users - Read & execute - This folder, subfolder, and files, Server Operators - Read & execute- This folder, subfolder, and files, Administrators - Special - This folder only (Special = Basic Permissions: all selected except Full control), CREATOR OWNER - Full control - Subfolders and files only, Administrators - Full control - Subfolders and files only, and SYSTEM - Full control - This folder, subfolders, and files

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224971
Rule ID: SV-224971r877392_rule
STIG ID: WN16-DC-000080
Severity: CAT I

20.11 Ensure 'Active Directory user accounts are configured to require the use of a Common Access Card (CAC), Personal Identity Verification (PIV)-compliant hardware token, or Alternate Logon Token (ALT)' (STIG DC only) (Manual)

Profile Applicability:

- STIG Domain Controller

Description:

This policy setting ensures that all Active Directory user accounts, including administrators, are configured to use a Common Access Card (CAC), Personal Identity Verification (PIV)-compliant hardware token, or Alternate Logon Token (ALT) for user authentication.

Rationale:

Requiring two-factor authentication provides a higher level of security, and therefore credentials are less likely to be compromised.

Impact:

Users will have to carry a form of two-factor authentication.

Audit:

Verify that Active Directory user accounts are configured to require the use of a Common Access Card (CAC), Personal Identity Verification (PIV)-compliant hardware token, or Alternate Logon Token (ALT):

- Open *PowerShell*
- Type *Get-ADUser -Filter {(Enabled -eq \$True) -and (SmartcardLogonRequired -eq \$False)} | FT Name* command (*DistinguishedName* may be substituted for *Name* for more detailed output)

If any user accounts, including administrators are listed, then this recommendation is not in compliance.

To check a single user account open *Active Directory Users and Computer* right click the user account and select properties, select the account tab, and ensure *Smart card is required for interactive logon* is checked.

Remediation:

To configure all user accounts, including administrator accounts in Active Directory to enable the option *Smart card is required for interactive logon*, do the following:

- Open *Active Directory Users and Computer*
- Right click the *user account* and select *properties*
- Select the *account tab*
- Ensure *Smart card is required for interactive logon* is checked

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224994
Rule ID: SV-224994r852363_rule
STIG ID: WN16-DC-000310
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.3 <u>Require MFA for Externally-Exposed Applications</u> Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.		●	●
v7	16.3 <u>Require Multi-factor Authentication</u> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

20.12 Ensure 'Administrative accounts cannot be used with applications that access the Internet, such as web browsers, or with potential Internet sources, such as email' (Manual)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting ensures that administrative accounts cannot be used with applications that access the Internet, such as web browsers, or with potential Internet sources, such as email.

Rationale:

Using applications that access the Internet or have potential Internet sources using administrative privileges exposes a system to compromise. If a flaw in an application is exploited while running as a privileged user, the entire system could be compromised. Web browsers and email are common attack vectors for introducing malicious code and must not be run with an administrative account.

Since administrative accounts may generally change or work around technical restrictions for running a web browser or other applications, it is essential that policy require administrative accounts to not access the Internet or use applications such as email.

Note: The policy should define specific exceptions for local service administration. These exceptions may include HTTP(S)-based tools that are used for the administration of the local system, services, or attached devices.

Note #2: Allow-listing can be used to enforce the policy to ensure compliance.

Impact:

Accounts with administrative privileges will not be able to access the Internet, such as web browsers, or with potential Internet sources, such as email.

Note: The policy should define specific exceptions for local service administration. These exceptions may include HTTP(S)-based tools that are used for the administration of the local system, services, or attached devices.

Note #2: Allow-listing can be used to enforce the policy to ensure compliance.

Audit:

Determine whether organization policy, at a minimum, prohibits administrative accounts from using applications that access the Internet, such as web browsers, or with potential Internet sources, such as email, except as necessary for local service administration.

Note: The organization may use technical means such as whitelisting to prevent the use of browsers and mail applications to enforce this requirement.

Remediation:

Establish a policy, at minimum, to prohibit administrative accounts from using applications that access the Internet, such as web browsers, or with potential Internet sources, such as email. Ensure the policy is enforced.

Note: The organization may use technical means such as whitelisting to prevent the use of browsers and mail applications to enforce this requirement.

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224821
Rule ID: SV-224821r569186_rule
STIG ID: WN16-00-000040
Severity: CAT I

20.13 Ensure 'Audit records must be backed up to a different system or media than the system being audited' (Manual)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting ensures that audit records are backed up to a different system or media than the system being audited.

Rationale:

Protection of log data includes assuring the log data is not accidentally lost or deleted. Audit information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Impact:

A secondary system that has enough resources to store large amounts of log data will be needed.

Audit:

Verify that audit records are backed up to a different system or media than the system being audited.

Remediation:

Establish and implement a process for backing up log data to another system or media other than the system being audited.

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224875
Rule ID: SV-224875r877390_rule
STIG ID: WN16-AU-000010
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.9 Centralize Audit Logs Centralize, to the extent possible, audit log collection and retention across enterprise assets.		●	●
v7	6.5 Central Log Management Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.		●	●

20.14 Ensure 'Automated mechanisms must be employed to determine the state of system components...' (Manual)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting ensures that automated mechanisms are in place to determine the state of system components regarding flaw remediation using the following frequency: **continuously, where Host Based Security System (HBSS) is used; 30 days, for any additional internal network scans not covered by HBSS; and annually, for external scans by Computer Network Defense Service Provider (CNDSP).**

Rationale:

Without the use of automated mechanisms to scan for security flaws on a continuous and/or periodic basis, the operating system or other system components may remain vulnerable to the exploits presented by undetected software flaws. The operating system may have an integrated solution incorporating continuous scanning using HBSS and periodic scanning using other tools.

Impact:

Automated mechanisms will need to be put in place to determine the state of system components. Resources for the system will need to be procured.

Audit:

Verify DoD approved HBSS software is installed, configured, and properly operating. Ask the operator to document the HBSS software installation and configuration. A documented configuration for an installed HBSS or if the HBSS software needs to be presented.

Remediation:

Install a DoD approved HBSS software and ensure it is operating continuously. In addition, a documented configuration for an installed HBSS or if the HBSS software needs to be created.

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224847
Rule ID: SV-224847r939261_rule
STIG ID: WN16-00-000320
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets</u> Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.			
v7	<u>3.1 Run Automated Vulnerability Scanning Tools</u> Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.			
v7	<u>3.2 Perform Authenticated Vulnerability Scanning</u> Perform authenticated vulnerability scanning with agents running locally on each system or with remote scanners that are configured with elevated rights on the system being tested.			

20.15 Ensure 'Data files owned by users must be on a different logical partition from the directory server data files' (STIG DC only) (Manual)

Profile Applicability:

- STIG Domain Controller

Description:

This policy setting ensures that data files that are owned by users are on a different logical partition from the directory server data files.

Rationale:

When directory service data files, especially for directories used for identification, authentication, or authorization, reside on the same logical partition as user-owned files, the directory service data may be more vulnerable to unauthorized access or other availability compromises. Directory service and user-owned data files sharing a partition may be configured with less restrictive permissions to allow access to the user data.

The directory service may be vulnerable to a denial-of-service attack when user-owned files on a common partition are expanded to an extent preventing the directory service from acquiring more space for directory or audit data.

Impact:

Multiple partitions must be created for the system.

Audit:

Navigate to the following registry key and note the directory locations in the values for *DSA Database file*.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters
```

- Open the *Command Prompt*
- Type *net share*

If user shares are located on the same logical partition as the directory server data files it is not in compliance with this recommendation.

Note: The logical drive(s) or file system partition for any organization-created data shares. Ignore system shares (e.g., NETLOGON, SYSVOL, and administrative shares ending in \$). User shares that are hidden (ending with \$) should not be ignored.

Remediation:

Move shares used to store files owned by users to a different logical partition than the directory server data files.

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224975
Rule ID: SV-224975r569186_rule
STIG ID: WN16-DC-000120
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

20.16 Ensure 'Default permissions for the HKEY_LOCAL_MACHINE registry hive must be maintained' (Manual)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting ensures that default permissions for the HKEY_LOCAL_MACHINE registry hive are maintained.

The recommended STIG state for this setting is:

HKEY_LOCAL_MACHINE\SECURITY SYSTEM - Full Control - This key and subkeys, and Administrators - Special - This key and subkeys;

HKEY_LOCAL_MACHINE\SOFTWARE Users - Read - This key and subkeys, Administrators - Full Control - This key and subkeys, SYSTEM - Full Control - This key and subkeys, CREATOR OWNER - Full Control - This key and subkeys, and ALL APPLICATION PACKAGES - Read - This key and subkeys;

HKEY_LOCAL_MACHINE\SYSTEM Administrators - Full Control - This key and subkeys, SYSTEM - Full Control - This key and subkeys, CREATOR OWNER - Full Control - Subkeys only, and ALL APPLICATION PACKAGES - Read - This key and subkeys

Rationale:

The registry is integral to the function, security, and stability of the Windows system. Changing the system's registry permissions allows the possibility of unauthorized and anonymous modification to the operating system.

Impact:

Non-privileged groups such as Users or Authenticated Users must not have greater than "Read" permissions except where noted as defaults. Individual accounts must not be used to assign permissions.

Audit:

Verify that the registry permissions for the keys of the HKEY_LOCAL_MACHINE hive noted below:

- Open *Regedit*
- Right-click on the registry areas noted below

Select *Permissions* and the *Advanced* button.

HKEY_LOCAL_MACHINE\SECURITY

Type - "Allow" for all

Inherited from - "None" for all

Principal - Access - Applies to:

SYSTEM - Full Control - This key and subkeys, and Administrators -
Special - This key and subkeys

HKEY_LOCAL_MACHINE\SOFTWARE

Type - "Allow" for all

Inherited from - "None" for all

Principal - Access - Applies to

Users - Read - This key and subkeys, Administrators - Full Control -
This key and subkeys, SYSTEM - Full Control - This key and subkeys,
CREATOR OWNER - Full Control - This key and subkeys, and ALL APPLICATION
PACKAGES - Read - This key and subkeys

HKEY_LOCAL_MACHINE\SYSTEM

Type - "Allow" for all

Inherited from - "None" for all

Principal - Access - Applies to

Users - Read - This key and subkeys

Administrators - Full Control - This key and subkeys, SYSTEM - Full
Control - This key and subkeys, CREATOR OWNER - Full Control - Subkeys
only, and ALL APPLICATION PACKAGES - Read - This key and subkeys

Note: Other examples under the noted keys may also be sampled. There may be some instances where non-privileged groups have greater than Read permission.

Note #2: Microsoft has given Read permission to the *SOFTWARE* and *SYSTEM* registry keys in Windows Server 2019 to the following SID: S-1-15-3-1024-1065365936-1281604716-3511738428-1654721687-432734479-3232135806-4053264122-3456934681 this is in compliance with the recommendation.

Remediation:

Maintain the default permissions for the registry keys of the HKEY_LOCAL_MACHINE hive as noted below.

- Open *Regedit*
- Right-click on the registry areas noted below

If the default settings are not present change the permissions to the following:
Select *Permissions* and the *Advanced* button.

HKEY_LOCAL_MACHINE\SECURITY

Type - "Allow" for all

Inherited from - "None" for all

Principal - Access - Applies to:

SYSTEM - Full Control - This key and subkeys, and Administrators -
Special - This key and subkeys

HKEY_LOCAL_MACHINE\SOFTWARE

Type - "Allow" for all

Inherited from - "None" for all

Principal - Access - Applies to

Users - Read - This key and subkeys, Administrators - Full Control -
This key and subkeys, SYSTEM - Full Control - This key and subkeys,
CREATOR OWNER - Full Control - This key and subkeys, and ALL APPLICATION
PACKAGES - Read - This key and subkeys

HKEY_LOCAL_MACHINE\SYSTEM

Type - "Allow" for all

Inherited from - "None" for all

Principal - Access - Applies to

Users - Read - This key and subkeys

Administrators - Full Control - This key and subkeys, SYSTEM - Full
Control - This key and subkeys, CREATOR OWNER - Full Control - Subkeys
only, and ALL APPLICATION PACKAGES - Read - This key and subkeys

Note: Microsoft has given Read permission to the *SOFTWARE* and *SYSTEM* registry keys in Windows Server 2019 to the following SID: S-1-15-3-1024-1065365936-1281604716-3511738428-1654721687-432734479-3232135806-4053264122-3456934681 this is in compliance with the recommendation.

Default Value:

HKEY_LOCAL_MACHINE\SECURITY

Type - "Allow" for all

Inherited from - "None" for all

Principal - Access - Applies to:

SYSTEM - Full Control - This key and subkeys, and Administrators -
Special - This key and subkeys

HKEY_LOCAL_MACHINE\SOFTWARE

Type - "Allow" for all

Inherited from - "None" for all

Principal - Access - Applies to

Users - Read - This key and subkeys, Administrators - Full Control -
This key and subkeys, SYSTEM - Full Control - This key and subkeys,
CREATOR OWNER - Full Control - This key and subkeys, and ALL APPLICATION
PACKAGES - Read - This key and subkeys

HKEY_LOCAL_MACHINE\SYSTEM

Type - "Allow" for all

Inherited from - "None" for all

Principal - Access - Applies to

Users - Read - This key and subkeys

Administrators - Full Control - This key and subkeys, SYSTEM - Full
Control - This key and subkeys, CREATOR OWNER - Full Control - Subkeys
only, and ALL APPLICATION PACKAGES - Read - This key and subkeys

Note: Microsoft has given Read permission to the *SOFTWARE* and *SYSTEM* registry
keys in Windows Server 2019 to the following SID: S-1-15-3-1024-1065365936-
1281604716-3511738428-1654721687-432734479-3232135806-4053264122-
3456934681 this is in compliance with the recommendation.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224835
Rule ID: SV-224835r877392_rule
STIG ID: WN16-00-000190
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

20.17 Ensure 'Deny-all, permit-by-exception policy to allow the execution of authorized software programs' (Manual)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting ensures that a deny-all, permit-by-exception policy is deployed to the system. This policy will only allow the execution of authorized software programs.

Note: The organization must identify authorized software programs and only permit execution of authorized software. The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as allow-listing.

Rationale:

Using an allow-list provides a configuration management method to allow the execution of only authorized software which can decrease the likelihood of malicious software executing on the system.

Impact:

Only authorized software will execute on the system.

Audit:

Verify that the operating system employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs.

Note: Configuration of allow-listing applications will vary by the program.

AppLocker is a allow-listing application that is built into the Windows Operating system. A deny-by-default implementation is initiated by enabling any AppLocker rules within a category, only allowing what is specified by defined rules.

If AppLocker is used on the system, perform the following to view the configuration of AppLocker:

- Open *PowerShell*
- Type *Get-AppLockerPolicy -Effective -XML > c:\temp\file.xml*, where [c:\temp\file.xml] is the location and file name appropriate for the system

This will produce an xml file with the effective settings that can be viewed in a browser or opened in a program such as Excel for review.

Note: If the AppLocker PowerShell module has not been imported previously, execute the following first:

Import-Module AppLocker

Remediation:

Configure an application allow-listing program to employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs.

If AppLocker is used, it is configured through group policy:

```
Computer Configuration\Windows Settings\Security Settings\Application Control Policies\AppLocker
```

Implementation guidance for AppLocker is available in the NSA paper: [Application Whitelisting using Microsoft AppLocker](#).

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224826
Rule ID: SV-224826r890501_rule
STIG ID: WN16-00-000090
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.5 Allowlist Authorized Software Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.		●	●
v7	2.7 Utilize Application Whitelisting Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.			●

20.18 Ensure 'Directory data (outside the root DSE) of a non-public directory is configured' (STIG DC only) (Manual)

Profile Applicability:

- STIG Domain Controller

Description:

This policy setting ensures that directory data outside of the root DSE of a non-public directory is configured to prevent anonymous access.

Rationale:

To the extent that anonymous access to directory data (outside the root DSE) is permitted, read access control of the data is effectively disabled. If other means of controlling access (such as network restrictions) are compromised, there may be nothing else to protect the confidentiality of sensitive directory data.

Impact:

Anonymous access to directory data outside the root DSE will not be permitted.

Audit:

Verify the following:

- Open *Command Prompt* (not elevated)
- Type *ldp.exe*
- From the *Connection menu*, select *Bind*
- Clear the User, Password, and Domain fields
- Select *Simple bind* for the Bind type and click OK

Confirmation of anonymous access will be displayed at the end:

res = ldap_simple_bind_s and Authenticated as: 'NT AUTHORITY\ANONYMOUS LOGON'

- From the *_Browse_menu*, select *Search*

In the Search dialog, enter the DN of the domain naming context (ex: dc=disaost,dc=mil) in the Base DN field.

- Clear the *Attributes* field and select *Run*

Error messages should display related to Bind and user not authenticated.

If attribute data is displayed, anonymous access is enabled to the domain naming context and this not in compliance.

The following network controls allow the finding severity to be downgraded to a CAT II since these measures lower the risk associated with anonymous access.

Network hardware ports at the site are subject to 802.1x authentication or MAC address restrictions.

Premise firewall or host restrictions prevent access to ports 389, 636, 3268, and 3269 from client hosts not explicitly identified by domain (.mil) or IP address.

Remediation:

Configure directory data outside the root DSE) of a non-public directory to prevent anonymous access.

For Active Directory, there are multiple configuration items that could enable anonymous access.

Changing the access permissions on the **domain naming context object** (from the secure defaults) could enable anonymous access. If the check procedures indicate this is the cause, the process that was used to change the permissions should be reversed. This could have been through the Windows Support Tools ADSI Edit console (adsiedit.msc).

The **dsHeuristics** option is used. This is addressed in check V-8555 in the Active Directory Forest STIG.

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224978
Rule ID: SV-224978r569186_rule
STIG ID: WN16-DC-000150
Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

20.19 Ensure 'Directory service must be configured to terminate LDAP-based network connections to the directory server after five minutes of inactivity' (STIG DC only) (Manual)

Profile Applicability:

- STIG Domain Controller

Description:

This policy setting ensures that the directory service is configured to terminate LDAP-based network connections to the directory server after five minutes of inactivity.

The STIG recommended state for this setting is: **300 (5 minutes) or less**.

Rationale:

Failure to terminate inactive network connections increases the risk of a successful attack on the directory server. The longer an established session is in progress, the more time an attacker has to hijack the session, implement a means to passively intercept data, or compromise any protections on client access. For example, if an attacker gains control of a client computer, an existing (already authenticated) session with the directory server could allow access to the directory. The lack of confidentiality protection in LDAP-based sessions increases exposure to this vulnerability.

Impact:

LDAP-based network connections to the directory server will terminate after five minutes of inactivity.

Audit:

Verify that LDAP-based network connections to the directory server will terminate after **300 (5 minutes) or less** of inactivity:

- Open an elevated *Command Prompt* (run as administrator)
- Type *ntdsutil*
- At the *ntdsutil*: prompt: type *LDAP policies*
- At the *ldap policy*: prompt: type *connections*
- At the *server connections*: prompt: type *connect to server [host-name]* (where [host-name] is the computer name of the domain controller)
- At the *server connections*: prompt, type *q*
- At the *ldap policy*: prompt, type *show values*

If the value for **MaxConnIdleTime** is greater than **300 (5 minutes)** or is not specified, it is not in compliance with this recommendation.

- Type *q* at the *ldap policy*: and *ntdsutil*: prompts to exit.

Remediation:

Configure the directory service to terminate LDAP-based network connections to the directory server after **300 (5 minutes) or less** of inactivity:

- Open an elevated *Command Prompt* (run as administrator), type *ntdsutil*
- At the *ntdsutil*: prompt: type *LDAP policies*
- At the *ldap policy*: prompt: type *connections*
- At the *server connections*: prompt: type *connect to server [host-name]* (where [host-name] is the computer name of the domain controller)
- At the *server connections*: prompt, type *q*
- At the *ldap policy*: prompt: type *Set MaxConnIdleTime to 300*
- Type *Commit Changes* to save
- Type *Show values* to verify changes
- Type *q* at the *ldap policy*: and *ntdsutil*: prompts to exit

Default Value:

120 seconds.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224979
Rule ID: SV-224979r569186_rule
STIG ID: WN16-DC-000160
Severity: CAT III

20.20 Ensure 'DoD Interoperability Root CA cross-certificates' are installed in the 'Untrusted Certificates Store' on unclassified systems (Manual)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting ensures that the DoD Interoperability Root CA cross-certificates are installed in the Untrusted Certificate Store on unclassified systems.

The STIG recommended state for this setting is: **DoD Root CA 3 - DoD Interoperability Root CA 2 - 49CBE933151872E17C8EAE7F0ABA97FB610F6477**

Rationale:

If the Interoperability Root CA cross-certificates are not installed in the Untrusted Certificates Store users may experience denial of service when performing certificate-based authentication to DoD websites due to the system chaining to a root other than DoD Root CAs.

Note: This requirement only applies to unclassified systems.

Impact:

N/A

Audit:

To establish the recommended configuration, navigate to the *Untrusted Certificate Store* to ensure the following certificates are installed:

DoD Root CA 3 - DoD Interoperability Root CA 2 - 49CBE933151872E17C8EAE7F0ABA97FB610F6477

Note: The Certificate Store can be loaded by executing the *Microsoft Management Console (MMC)* and loading the *Certificates* snap-in.

Remediation:

Install the following DoD Root CA certificates in the *Untrusted Certificates Store*:

DoD Root CA 3 - DoD Interoperability Root CA 2 -
49CBE933151872E17C8EAE7F0ABA97FB610F6477

Note: The InstallRoot tool is available on IASE at <http://iase.disa.mil/pki-pke/Pages/tools.aspx>.

Note #2: The Certificate Store can be loaded by executing the *Microsoft Management Console (MMC)* and loading the *Certificates* snap-in.

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225022
Rule ID: SV-225022r894338_rule
STIG ID: WN16-PK-000020
Severity: CAT II

20.21 Ensure 'DoD Root Certificate Authority (CA) certificates' are installed in the 'Trusted Root Store' (Manual)

Profile Applicability:

- STIG Member Server
- STIG Domain Controller

Description:

This policy setting ensures that the DoD Root CA certificates are installed in the Trusted Root Store to secure DoD websites and to ensure DoD-signed code is properly validated.

The STIG recommended state for this setting is: DoD Root CA 3, DoD Root CA 4, DoD Root CA 5, and DoD Root CA 6.

Rationale:

DoD root certificates will ensure that the trust chain is established for server certificates issued from the DoD CAs.

Impact:

N/A

Audit:

To establish the recommended configuration, navigate to the *Trusted Certificate Store* to ensure the following certificates are installed:

DoD Root CA 3, **DoD Root CA 4**, **DoD Root CA 5**, and **DoD Root CA 6**

With the *Value* for the thumbprint filed as followed:

DoD Root CA 3

Thumbprint: D73CA91102A2204A36459ED32213B467D7CE97FB

Valid to: December 30, 2029

DoD Root CA 4

Thumbprint: B8269F25DBD937ECAFD4C35A9838571723F2D026

Valid to: July 25, 2032

DoD Root CA 5

Thumbprint: 4ECB5CC3095670454DA1CBD410FC921F46B8564B

Valid to: June 14, 2041

DoD Root CA 6

Thumbprint: D37ECF61C0B4ED88681EF3630C4E2FC787B37AEF

Valid to: January 24, 2053

Note: The Certificate Store can be loaded by executing the *Microsoft Management Console (MMC)* and loading the *Certificates* snap-in.

Remediation:

Install the following DoD Root CA certificates in the *Trusted Certificates Store*:

DoD Root CA 3, DoD Root CA 4, DoD Root CA 5, and DoD Root CA 6

With the *Value* for the thumbprint filed as followed:

DoD Root CA 3, DoD Root CA 4, DoD Root CA 5, and DoD Root CA 6

With the *Value* for the thumbprint filed as followed:

DoD Root CA 3

Thumbprint: D73CA91102A2204A36459ED32213B467D7CE97FB

Valid to: December 30, 2029

DoD Root CA 4

Thumbprint: B8269F25DBD937ECAFD4C35A9838571723F2D026

Valid to: July 25, 2032

DoD Root CA 5

Thumbprint: 4ECB5CC3095670454DA1CBD410FC921F46B8564B

Valid to: June 14, 2041

DoD Root CA 6

Thumbprint: D37ECF61C0B4ED88681EF3630C4E2FC787B37AEF

Valid to: January 24, 2053

Note: The InstallRoot tool is available on IASE at <http://iase.disa.mil/pki-pke/Pages/tools.aspx>.

Note #2: The Certificate Store can be loaded by executing the *Microsoft Management Console (MMC)* and loading the *Certificates* snap-in.

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225021
Rule ID: SV-225021r953814_rule
STIG ID: WN16-PK-000010
Severity: CAT II

20.22 Ensure 'Domain Controller PKI certificates must be issued by the DoD PKI or an approved External Certificate Authority' (STIG DC only) (Manual)

Profile Applicability:

- STIG Domain Controller

Description:

This policy setting ensures that Domain Controller Public Key Infrastructure (PKI) certificates are issued by the DoD PKI or an approved External Certificate Authority (ECA).

Rationale:

The use of multiple CAs from separate PKI implementations results in interoperability issues and if servers and clients do not have a common set of root CA certificates, they will not be able to authenticate each other.

Impact:

Only authorized CA certificates are allowed.

Audit:

To establish the recommended configuration, navigate to the *Certificate Store* to ensure the certificates are issued by the DoD PKI or an approved ECA.

The *Certificate Store* can be loaded by executing the *Microsoft Management Console (MMC)* and loading the *Certificates* snap-in (Computer account). Expand the certificates and ensure the **personal** entry is DoD PKI or an approved ECA.

Remediation:

Install DoD PKI or an approved ECA certificates.

Note: The [Global Directory Service \(GDS\)](#) website provides an online source for approved certificates.

Note #2: DoD Public Key Enablement (PKE) Engineering Support maintains the InstallRoot utility to manage DoD supported root certificates on Windows computers, which includes a list of authorized CAs. The utility package can be downloaded from the [PKI and PKE Tools](#) page on IASE.

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224992
Rule ID: SV-224992r569186_rule
STIG ID: WN16-DC-000290
Severity: CAT I

20.23 Ensure 'Domain controllers have a PKI server certificate' (STIG DC only) (Manual)

Profile Applicability:

- STIG Domain Controller

Description:

This policy setting ensures that Domain controllers have a server certificate to establish authenticity as part of PKI authentications in the domain.

Rationale:

Domain controllers are part of the chain of trust for PKI authentications. Without the appropriate certificate, the authenticity of the domain controller cannot be verified.

Impact:

Without the appropriate certificate, the authenticity of the domain controller cannot be verified.

Audit:

To establish the recommended configuration, navigate to the *Certificate Store* to ensure that a server certificate is issued to the Domain Controller by the DoD PKI or an approved ECA.

The *Certificate Store* can be loaded by executing the *Microsoft Management Console (MMC)* and loading the *Certificates* snap-in (Computer account). Expand the certificates and ensure a Domain Controller certificate is present in the **personal** directory.

Remediation:

If no certificate exists, install an approved certificate on the Domain Controller.

Note: The *Certificate Store* can be loaded by executing the *Microsoft Management Console (MMC)* and loading the *Certificates* snap-in (Computer account).

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224991
Rule ID: SV-224991r569186_rule
STIG ID: WN16-DC-000280
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

20.24 Ensure 'Domain Controllers run on a machine dedicated to that function' (STIG DC only) (Manual)

Profile Applicability:

- STIG Domain Controller

Description:

This policy setting ensures that Domain Controllers are run on a system that is dedicated to Domain Controller functions only.

Rationale:

Executing application servers on the same host machine with a directory server may substantially weaken the security of the directory server. Web or database server applications usually require the addition of many programs and accounts, increasing the attack surface of the computer.

In addition, some applications require the addition of privileged accounts, providing potential sources of compromise. Some applications (such as Microsoft Exchange) may require the use of network ports or services conflicting with the directory server. In this case, non-standard ports might be selected, and this could interfere with intrusion detection or prevention services.

Impact:

A system must be dedicated to the Domain Controller and cannot have other applications, Roles and Features, or Programs and Features installed.

Audit:

Review the installed roles on the Domain Controller by doing the following:

- Open *Server Manager*
- Select *AD DS* in the left pane
- Select the server name under *Servers*
- Select *Add (or Remove) Roles and Features* from *Tasks* in the *Roles and Features* section

Determine if any server roles are installed. A basic domain controller setup will include the following:

- Active Directory Domain Services
- DNS Server
- File and Storage Services

Cancel out of *Roles and Features* before any changes are made.

AND

Run *Programs and Features*.

Determine if any *Programs and Features* are installed that are not needed on the domain controller.

If *Roles and Features* or *Programs and Features* that are not required on a domain controller are installed it is not in compliance with this recommendation.

Note: A Domain Name System (DNS) server integrated with the directory server (e.g., AD-integrated DNS) is an acceptable application. However, the DNS server must comply with the DNS STIG security requirements.

Remediation:

Remove any *Roles and Features* or *Programs and Features* that are not required for the domain controller to function.

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224976
Rule ID: SV-224976r569186_rule
STIG ID: WN16-DC-000130
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

20.25 Ensure 'Domain-joined systems have a Trusted Platform Module (TPM) enabled and ready for use' (Manual)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting ensures that all domain-joined systems have a Trusted Platform Module (TPM) enabled and ready for use.

Note: This recommendation does not apply to stand-alone systems.

Rationale:

Credential Guard uses virtualization-based security to protect data that could be used in credential theft attacks if compromised. Several system requirements must be met in order for Credential Guard to be configured and enabled properly. Without a TPM enabled and ready for use, Credential Guard keys are stored in a less secure method using software.

Impact:

Systems without a Trusted Platform Module (TPM) enabled are not authorized.

Audit:

Verify the system has a TPM and it is ready for use:

Execute *tpm.msc*, review the sections in the center pane. The *Status* must indicate it has been configured with a message such as *The TPM is ready for use* or *The TPM is on and ownership has been taken*. **TPM Manufacturer Information - Specific Version = 2.0 or 1.2.**

Note: Current hardware and virtual environments may not support virtualization-based security features, including Credential Guard, due to specific supporting requirements including a TPM, UEFI with Secure Boot, and the capability to run the Hyper-V feature within a virtual machine.

Remediation:

Ensure that domain-joined systems have a TPM that is configured for use. (Versions 2.0 or 1.2 support Credential Guard.)

Execute *tpm.msc* for configuration options in the Windows Operating System.

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224827
Rule ID: SV-224827r902425_rule
STIG ID: WN16-00-000100
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

20.26 Ensure 'Emergency accounts must be automatically removed or disabled after the crisis is resolved or within 72 hours' (Manual)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting ensures that emergency accounts are automatically remove or disabled after the crisis is resolved or within 72 hours of the crisis.

Rationale:

Emergency administrator accounts are privileged accounts established in response to crisis situations where the need for rapid account activation is required. Therefore, emergency account activation may bypass normal account authorization processes. If these accounts are automatically disabled, system maintenance during emergencies may not be possible, thus adversely affecting system availability.

Emergency administrator accounts are different from infrequently used accounts (i.e., local logon accounts used by system administrators when network or normal logon/access is not available). Infrequently used accounts are not subject to automatic termination dates. Emergency accounts are accounts created in response to crisis situations, usually for use by maintenance personnel. The automatic expiration or disabling time period may be extended as needed until the crisis is resolved; however, it must not be extended indefinitely. A permanent account should be established for privileged users who need long-term maintenance accounts.

To address access requirements, many operating systems can be integrated with enterprise-level authentication/access mechanisms that meet or exceed access control policy requirements.

Impact:

Emergency administrator accounts are not authorized to be enabled after the crisis is complete.

Audit:

Verify if emergency administrator accounts are used and identify any that exist:

Domain Controller:

- Open *PowerShell*
- Type *Search-ADAccount -AccountExpiring | FT Name, AccountExpirationDate*

If **AccountExpirationDate** has been defined and is not within 72 hours for an emergency administrator account, this is a finding.

Member servers/Stand-alone systems:

- Open the *Command Prompt*
- Type *Net user [username]* where [username] is the name of the emergency account.

If **Account expires** has been defined and is not within 72 hours for an emergency administrator account, this is a finding.

If emergency administrator accounts cannot be configured with an expiration date due to an ongoing crisis, the accounts must be disabled or removed when the crisis is resolved.

If emergency administrator accounts have not been configured with an expiration date or have not been disabled or removed following the resolution of a crisis, this is a finding.

Remediation:

Remove any emergency administrator accounts after a crisis has been resolved or configure the accounts to automatically expire within 72 hours.

Domain accounts can be configured with an account expiration date, under *Account* properties.

Local accounts can be configured to expire with the following command:

- Open the *Command Prompt*
- Type *Net user [username] /expires:[mm/dd/yyyy]* where username is the name of the temporary user account

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224849
Rule ID: SV-224849r857243_rule
STIG ID: WN16-00-000340
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.3 <u>Disable Dormant Accounts</u> Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.			
v7	16.8 <u>Disable Any Unassociated Accounts</u> Disable any account that cannot be associated with a business process or business owner.			

20.27 Ensure 'Event Viewer must be protected from unauthorized modification and deletion' (Manual)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This setting restricts permissions to the Event Viewer, which is used to view and manipulate log data.

The STIG recommended state for this setting is: **TrustedInstaller - Full Control, Administrators - Read & Execute, SYSTEM - Read & Execute, Users - Read & Execute, ALL APPLICATION PACKAGES - Read & Execute, and ALL RESTRICTED APPLICATION PACKAGES - Read & Execute.**

Rationale:

Protecting audit information also includes identifying and protecting the tools used to view and manipulate log data. Therefore, protecting audit tools is necessary to prevent unauthorized operation of audit information.

Impact:

Users will be able to open Event Viewer and view logs, but not able to delete logs.

Audit:

Navigate to the path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration, set the NTFS permissions on the file below to **TrustedInstaller - Full Control, Administrators - Read & Execute, SYSTEM - Read & Execute, Users - Read & Execute, ALL APPLICATION PACKAGES - Read & Execute, and ALL RESTRICTED APPLICATION PACKAGES - Read & Execute:**

%SystemRoot%\ System32\Eventvwr.exe

Default Value:

TrustedInstaller - Full Control, Administrators - Read & Execute, SYSTEM - Read & Execute, Users - Read & Execute, ALL APPLICATION PACKAGES - Read & Execute, and ALL RESTRICTED APPLICATION PACKAGES - Read & Execute

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224880
Rule ID: SV-224880r569186_rule
STIG ID: WN16-AU-000060
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

20.28 Ensure 'Fax Server role' is set to 'Not Installed' (Manual)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This setting provides a single interface that administrators can use to efficiently administer fax resources.

The STIG recommended state for this setting is: **Not installed**

Note: A fax server is comprised of four different parts:

- Fax Server role
- Fax service
- Fax Service Manager
- Windows Fax and Scan

Rationale:

Unnecessary services increase the attack surface of a system. Some of these services may not support required levels of authentication or encryption or may provide unauthorized access to the system.

Impact:

Fax Server features such as automatically making fax connections available to users and computers in your organization will not be possible.

Audit:

Navigate to the path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To Uninstall the *Fax Server* role:

- Start "Server Manager"
- Select the server with the role
- Scroll down to "ROLES AND FEATURES" in the right pane
- Select "Remove Roles and Features" from the drop-down "TASKS" list
- Select the appropriate server on the "Server Selection" page and click "Next"
- Deselect "Fax Server" on the "Roles" page
- Click "Next" and "Remove" as prompted (if installed).

Default Value:

Not installed.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224850
Rule ID: SV-224850r569186_rule
STIG ID: WN16-00-000350
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			

20.29 Ensure 'FTP servers are configured to prevent access to the system drive' (Manual)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting ensures that File Transfer Protocol (FTP) servers are configured to prevent access to the system drive.

Rationale:

The FTP service allows remote users to access shared files and directories that could provide access to system resources and compromise the system, especially if the user can gain access to the root directory of the boot drive.

Impact:

The system drive will not be accessible through FTP.

Audit:

Verify that the FTP role is not installed on the system:

- Open *Internet Information Services (IIS) Manager*
- Select *Sites* under the server name.
- For any sites with a *Binding* that lists *FTP*: right-click the site and select *Explore*

If the site is not defined to a specific folder for shared FTP resources, this is a finding. If the site includes any system areas such as root of the drive, Program Files, or Windows directories, this is a finding.

Remediation:

Configure the FTP sites to allow access only to specific FTP shared resources. Do not allow access to other areas of the system.

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224861
Rule ID: SV-224861r569186_rule
STIG ID: WN16-00-000440
Severity: CAT II

20.30 Ensure 'FTP servers must be configured to prevent anonymous logons' (Manual)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting ensures that File Transfer Protocol (FTP) servers are configured to prevent anonymous logons.

The STIG recommended state for this setting is: **Disabled**.

Rationale:

The FTP service allows remote users to access shared files and directories. Allowing anonymous FTP connections makes user auditing difficult and can allow attackers to gain access to data and store malware and launch attacks from the system.

Impact:

Using accounts that have administrator privileges to log on to FTP risks that the userid and password will be captured on the network and give administrator access to an unauthorized user.

Audit:

Verify that FTP is not installed:

- Open *Internet Information Services (IIS) Manager*
- Select the *server*, double-click *FTP Authentication*
- Select *Anonymous Authentication*

Ensure **Anonymous Authentication** is set to **Disabled**.

Remediation:

To configure the *FTP service* to prevent anonymous logons:

- Open *Internet Information Services (IIS) Manager*
- Select the *server*
- Double-click *FTP Authentication*
- Select *Anonymous Authentication*
- Select **Disabled** under *Actions*

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224860
Rule ID: SV-224860r569186_rule
STIG ID: WN16-00-000430
Severity: CAT II

20.31 Ensure 'Host-based firewall is installed and enabled' (Manual)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting ensures that a host-based firewall is installed and enabled on the system.

The STIG recommended state for this setting is: **Installed** and **Enabled**

Rationale:

A firewall provides a line of defense against attack, allowing or blocking inbound and outbound connections based on a set of rules.

Impact:

Some system features might be blocked by the Firewall if it's not properly configured.

Audit:

Verify that a host-based firewall is installed and enabled on the system.

Note: The configuration requirements will be determined by the applicable Firewall Security Technical Implementation Guide (STIG).

Remediation:

Install and enable a host-based firewall on the system.

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224846
Rule ID: SV-224846r852299_rule
STIG ID: WN16-00-000310
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.			
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			

20.32 Ensure 'krbtgt account password' is no more than '180 days old' (STIG DC only) (Manual)

Profile Applicability:

- STIG Domain Controller

Description:

This policy setting ensures that the krbtgt account which acts as a service account for the Kerberos Key Distribution Center (KDC) service is no more than 180 days old. This account is created when a domain is created.

The STIG recommended state for this setting is: **No more than 180 days old**.

Rationale:

If the krbtgt account is compromised, attackers can create valid Kerberos Ticket Granting Tickets (TGT).

Impact:

The krbtgt account password will need to be changed manually every 180 days.

Audit:

Verify that the *krbtgt* account password is no more than **180 days old**

- Open PowerShell
- Type `Get-ADUser krbtgt -Property PasswordLastSet`

If the **PasswordLastSet** date is more than **180 days old**, it is not in compliance with this recommendation.

Remediation:

Reset the krbtgt account password via PowerShell. PowerShell scripts to reset the password can be found at the following Microsoft webpage: [Browse code samples | Microsoft Docs](#)

Note: The password must be changed twice to effectively remove the password history. Changing the password once and waiting for replication to complete and then changing again reduces the risk of issues. Changing the password twice in rapid succession forces clients to re-authenticate (including application services) but is desired if a compromise is suspected.

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225006
Rule ID: SV-225006r569186_rule
STIG ID: WN16-DC-000430
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16.10 <u>Ensure All Accounts Have An Expiration Date</u> Ensure that all accounts have an expiration date that is monitored and enforced.			

20.33 Ensure 'Local volumes must use a format that supports NTFS attributes' (Manual)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting ensures that volumes are formatted to use NT file system (NTFS) or Resilient File System (ReFS).

Note: The (ReFS) file system is a Microsoft proprietary file system introduced with Windows Server 2012 with the intent of becoming the "next generation" file system after NTFS.

Rationale:

The ability to set access permissions and auditing is critical to maintaining the security and proper access controls of a system. To support this, volumes must be formatted using a file system that supports NTFS attributes.

Impact:

Only NTFS or ReFS file systems are authorized for a volume.

Audit:

Verify that the file system uses *NTFS* or *ReFS*

- Open *Computer Management*
- Select *Disk Management* under *Storage*

For each local volume, verify that the file system indicates *NTFS* or *ReFS*.

Note: This does not apply to system partitions such the Recovery and EFI System Partition.

Remediation:

Format volumes to use NTFS or ReFS.

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224831
Rule ID: SV-224831r569186_rule
STIG ID: WN16-00-000150
Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

20.34 Ensure 'Manually managed application account passwords are 14 characters in length' (Manual)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting ensures that all manually managed application account passwords are at least 14 characters in length.

The recommended STIG state for this setting is: **14 or more characters**.

Rationale:

Application account passwords must be of sufficient length to prevent being easily cracked. Application accounts that are manually managed must have passwords at least 14 characters in length.

Impact:

All manually managed accounts will need to be at least 14 characters in length.

Audit:

Verify if manually managed application accounts exist and are at **14 characters or more**.

Verify the organization has a policy to ensure passwords for manually managed application accounts are at least 14 characters in length.

Remediation:

Establish a policy that requires application/service account passwords that are manually managed to be **14 characters or more** in length. Ensure that the policy is enforced.

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224823
Rule ID: SV-224823r953812_rule
STIG ID: WN16-00-000060
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			

20.35 Ensure 'Manually managed application account passwords be changed at least annually or when a system administrator with knowledge of the password leaves the organization' (Manual)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting ensures that all manually managed application account passwords are changed at least annually or when a system administrator with knowledge of the password leaves the organization.

Rationale:

Setting application account passwords to expire may cause applications to stop functioning. However, not changing them on a regular basis exposes them to attack. If managed service accounts are used, this alleviates the need to manually change application account passwords.

Impact:

Manually managed application account passwords will need to be changed at least annually.

Audit:

Verify that manually managed application account passwords are changed at least annually or when a system administrator with knowledge of the password leaves the organization:

Domain controllers:

- Open *PowerShell*
- Type *Get-AdUser -Identity [application account name] -Properties PasswordLastSet | FT Name, PasswordLastSet*, where [application account name] is the name of the manually managed application/service account

Ensure the **PasswordLastSet** date is no more than **one year old**.

Member servers and standalone systems:

- Open the *Command Prompt*
- Type *Net User [application account name] | Find /i "Password Last Set"*, where [application account name] is the name of the manually managed application/service account

Ensure the **PasswordLastSet** date is no more than **one year old**.

Remediation:

Change passwords for manually managed application/service accounts at least annually or when an administrator with knowledge of the password leaves the organization.

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224824
Rule ID: SV-224824r857226_rule
STIG ID: WN16-00-000070
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16.10 <u>Ensure All Accounts Have An Expiration Date</u> Ensure that all accounts have an expiration date that is monitored and enforced.		●	●

20.36 Ensure 'Members of the Backup Operators group have separate accounts for backup duties and normal operational tasks' (Manual)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting ensures that members of the Backup Operators group have separate accounts for backup duties and normal operational tasks.

Rationale:

Backup Operators can read and write to any file in the system, regardless of the rights assigned to it. Backup and restore rights permit users to circumvent the file access restrictions present on NTFS disk drives for backup and restore purposes. Members of the Backup Operators group must have separate logon accounts for performing backup duties.

Impact:

Members of the Backup Operators group will not be able to use the account associated with the Backup Operators group for standard user tasks.

Audit:

Verify users with accounts in the Backup Operators group have a separate user account for backup functions and for performing standard user tasks.

Note: If no accounts are members of the Backup Operators group, this recommendation N/A.

Remediation:

Ensure each member of the Backup Operators group has separate accounts for backup functions and standard user functions.

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224822
Rule ID: SV-224822r569186_rule
STIG ID: WN16-00-000050
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 <u>Restrict Administrator Privileges to Dedicated Administrator Accounts</u> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.			
v7	4.3 <u>Ensure the Use of Dedicated Administrative Accounts</u> Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.			

20.37 Ensure 'Non-administrative accounts or groups only have print permissions on printer shares' (Manual)

Profile Applicability:

- STIG Member Server
- STIG Domain Controller

Description:

This policy setting ensures that non-administrative accounts or groups only have print permissions on printer shares.

Rationale:

Windows shares are a means by which files, folders, printers, and other resources can be published for network users to access. Improper configuration can permit access to devices and data beyond a user's need.

Impact:

Standard user accounts will only have print permissions on printer shares.

Audit:

Verify that standard user accounts only have print permissions on printer shares.

Open *Printers & scanners* in *Settings*.

If there are no printers configured, this is NA. (Exclude Microsoft Print to PDF and Microsoft XPS Document Writer, which do not support sharing.)

For each printer:

- Select the *printer*
- Select *Manage*
- Select *Printer Properties*
- Select the *Sharing* tab

If **Share this printer** is checked, select the *Security* tab.

If any standard user accounts or groups have permissions other than "Print", this does not conform with this recommendation.

The default is for the **Everyone** group to be given *Print* permission.

Note: **ALL APPLICATION PACKAGES** and **CREATOR OWNER** are not standard user accounts.

Remediation:

Configure the permissions on shared printers to restrict standard users to only have Print permissions.

Open *Printers & scanners* in *Settings*.

For each printer:

- Select the *printer*
- Select *Manage*
- Select *Printer Properties*
- Select the *Sharing* tab

If **Share this printer** is checked, select the *Security* tab and change the permissions.

Default Value:

Everyone group - *Print* permissions.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224836
Rule ID: SV-224836r569186_rule
STIG ID: WN16-00-000200
Severity: CAT III

20.38 Ensure 'Non-system-created file shares must limit access to groups that require it' (Manual)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting ensures that non-system-created file shares limit access to groups that require it.

Rationale:

Shares on a system provide network access. To prevent exposing sensitive information, where shares are necessary, permissions must be reconfigured to give the minimum access to accounts that require it.

Impact:

Shares will be locked down to Users/Groups that need access.

Audit:

Verify that permissions have been configured to restrict permissions to the specific groups or accounts that require access.

- Run *Computer Management*
- Navigate to *System Tools > Shared Folders > Shares*
- Right-click any *non-system-created shares*
- Select *Properties*
- Select the *Share Permissions* tab
- Select the *Security* tab

Note: If only system-created shares such as **ADMIN\$**, **C\$**, and **IPC\$** exist on the system, this is NA. (System-created shares will display a message that it has been shared for administrative purposes when "Properties" is selected.)

Remediation:

If a non-system-created share is required on a system, configure the share and NTFS permissions to limit access to the specific groups or accounts that require it. Remove any unnecessary non-system-created shares.

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224841
Rule ID: SV-224841r569186_rule
STIG ID: WN16-00-000250
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	14.6 <u>Protect Information through Access Control Lists</u> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

20.39 Ensure 'Off-load of audit records of interconnected systems in real time and off-load standalone systems weekly' (Manual)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting ensures that at a minimum, audit records of interconnected systems are off-loaded in real time and stand-alone system audit records are off-loaded at least weekly.

Rationale:

Protection of log data includes assuring the log data is not accidentally lost or deleted. Audit information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Impact:

A secondary system that has enough resources to store large amounts of log data will be needed.

Audit:

Verify that audit records for interconnected systems are off-loaded in real time and stand-alone systems are off- weekly.

Remediation:

Configure the system to, at a minimum, off-load audit records of interconnected systems in real time and off-load standalone systems weekly.

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224876
Rule ID: SV-224876r860019_rule
STIG ID: WN16-AU-000020
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.9 <u>Centralize Audit Logs</u> Centralize, to the extent possible, audit log collection and retention across enterprise assets.			
v7	6.5 <u>Central Log Management</u> Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.			

20.40 Ensure 'Only Administrators have Administrator rights on the system' (STIG MS only) (Manual)

Profile Applicability:

- STIG Member Server

Description:

This policy setting ensures that only authorized Administrators responsible for the system have administrator rights.

The STIG recommended state for this setting is: **Authorized Administrators**

Rationale:

A standard user account should not have administrator rights on a system. Having these rights could allow the account, if compromised, to bypass or modify required security restrictions on that machine.

Impact:

Standard user accounts must not be members of the domain and built-in Administrators group.

Audit:

Verify that only authorized Administrators responsible for the system have administrator rights.

Stand-alone system

- Open *Local Users and Groups*
- Navigate to *Groups*
- Review the **Administrators** group for unauthorized accounts or standard user accounts that should not have administrator privileges.

Domain-joined system

- Open *Active Directory Users and Computers*
- Review the **Administrators** and **Domain Admins** groups (which must be replaced with a domain member server administrator group) group for unauthorized accounts or standard user accounts that should not have administrator privileges.

Remediation:

Remove any unauthorized or standard user accounts from the **Administrators** group.

Stand-alone system

- Open *Local Users and Groups*
- Navigate to *Groups*
- Review the **Administrators** group for unauthorized accounts or standard user accounts that should not have administrator privileges.

Remove any unauthorized or standard user accounts.

Domain-joined system

- Open *Active Directory Users and Computers*
- Review the **Administrators** and **Domain Admins** groups (which must be replaced with a domain member server administrator group) group for unauthorized accounts or standard user accounts that should not have administrator privileges.

Remove any unauthorized or standard user accounts.

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225007
Rule ID: SV-225007r877392_rule
STIG ID: WN16-MS-000010
Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</u> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.			
v7	<u>4.3 Ensure the Use of Dedicated Administrative Accounts</u> Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.			

20.41 Ensure 'Only administrators responsible for the Domain Controller to have Administrator rights on the system' (STIG DC only) (Manual)

Profile Applicability:

- STIG Domain Controller

Description:

This policy setting ensures that only administrators responsible for Domain Controllers have Administrator rights on the system.

Rationale:

An account that does not have Administrator duties must not have Administrator rights. Such rights would allow the account to bypass or modify required security restrictions on that machine and make it vulnerable to attack.

Impact:

Only users that administrator rights will have administrator rights.

Audit:

Verify that only appropriate administrator groups or accounts responsible for administration of the system are members of the Administrators group (domain and built-it/local).

Stand-alone system

- Open *Local Users and Groups*
- Select *Groups* and review the **Administrators** group for unauthorized accounts or standard user accounts that should not have administrator privileges.

Domain-joined system

- Open *Active Directory Users and Computers* and review the **Administrators** group for unauthorized accounts or standard user accounts that should not have administrator privileges.

Remediation:

Remove any unauthorized or standard user accounts from the **Administrators** group.

Stand-alone system

- Open *Local Users and Groups*
- Select *Groups* and review the **Administrators** group for unauthorized accounts or standard user accounts that should not have administrator privileges.

Remove any unauthorized or standard user accounts.

Domain-joined system

- Open *Active Directory Users and Computers* and review the **Administrators** group for unauthorized accounts or standard user accounts that should not have administrator privileges.

Remove any unauthorized or standard user accounts.

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224964
Rule ID: SV-224964r569186_rule
STIG ID: WN16-DC-000010
Severity: CAT I

20.42 Ensure 'Operating System is maintained at a supported servicing level' (Manual)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting ensures that the Operating System is maintained at a supported servicing level.

Rationale:

Systems at unsupported servicing levels will not receive security updates for new vulnerabilities, which leave them subject to exploitation. Systems must be maintained at a servicing level supported by the vendor with new security updates.

Impact:

The Windows Operating System must be at least **Microsoft Windows Server Version 1809 (Build 17763.xxx:)** or newer.

Audit:

Verify that the operating system is at least **Microsoft Windows Server Version 1809 (Build 17763.xxx:)** or newer.

- Open *Command Prompt*
- Type *winver.exe*

Ensure that the "About Windows" dialog box displays "Microsoft Windows Server Version 1809 (Build 17763.xxx)" or greater.

Remediation:

Update the system to a **Version 1809 (Build 17763.xxx)** or newer.

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224828
Rule ID: SV-224828r569186_rule
STIG ID: WN16-00-000110
Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.2 <u>Ensure Authorized Software is Currently Supported</u> Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.			
v7	2.2 <u>Ensure Software is Supported by Vendor</u> Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.			

20.43 Ensure 'Organization created Active Directory Organizational Unit (OU) objects have proper access control permissions' (STIG DC only) (Manual)

Profile Applicability:

- STIG Domain Controller

Description:

This policy setting ensures that Active Directory Organizational Unit (OU) objects that are created by the organization have proper access control permissions.

The recommended STIG state for this setting is: **CREATOR OWNER - Special permissions, Self - Special permissions, Authenticated Users - Read, Special permissions, SYSTEM - Full Control, Domain Admins - Full Control, Enterprise Admins - Full Control, Key Admins - Special permissions, Enterprise Key Admins - Special permissions, Administrators - Read, Write, Create all child objects, Generate resultant set of policy (logging), Generate resultant set of policy (planning), Special permissions, Pre-Windows 2000 Compatible Access - Special permissions, and ENTERPRISE DOMAIN CONTROLLERS - Read, Special permissions**

Note: The special permissions for Authenticated Users are Read type.

Note #2: The special permissions for Pre-Windows 2000 Compatible Access are for Read types.

Rationale:

When directory service database objects do not have appropriate access control permissions, it may be possible for malicious users to create, read, update, or delete the objects and degrade or destroy the integrity of the data. When the directory service is used for identification, authentication, or authorization functions, a compromise of the database objects could lead to a compromise of all systems that rely on the directory service.

For Active Directory, the OU objects require special attention. In a distributed administration model (i.e., help desk), OU objects are more likely to have access permissions changed from the secure defaults. If inappropriate access permissions are defined for OU objects, it could allow an intruder to add or delete users in the OU. This could result in unauthorized access to data or a denial of service (DoS) to authorized users.

Impact:

Only authorized users will have access control permissions.

Audit:

Verify access control permissions on organization-defined OUs:

- Open *Active Directory Users and Computers*
- Ensure *Advanced Features* is selected in the *View* menu

For each OU that is defined (folder in folder icon) excluding the Domain Controllers OU:

- Right-click the OU and select *Properties*
- Select the *Security* tab

If the **Allow** type permissions on the OU are not at least as restrictive as those below it is not in compliance with this recommendation.

The permissions shown are at the summary level. More detailed permissions can be viewed by selecting the *Advanced* button, the desired Permission entry, and the *Edit* or *View* button.

CREATOR OWNER - Special permissions, Self - Special permissions, Authenticated Users - Read, Special permissions, SYSTEM - Full Control, Domain Admins - Full Control, Enterprise Admins - Full Control, Key Admins - Special permissions, Enterprise Key Admins - Special permissions, Administrators - Read, Write, Create all child objects, Generate resultant set of policy (logging), Generate resultant set of policy (planning), Special permissions, Pre-Windows 2000 Compatible Access - Special permissions, and ENTERPRISE DOMAIN CONTROLLERS - Read, Special permissions.

If an ISSO-approved distributed administration model (help desk or other user support staff) is implemented, permissions above Read may be allowed for groups documented by the ISSO.

If any OU with improper permissions includes identification or authentication data (e.g., accounts, passwords, or password hash data) used by systems to determine access control, the severity is CAT I (e.g., OUs that include user accounts, including service/application accounts).

If an OU with improper permissions does not include identification and authentication data used by systems to determine access control, the severity is CAT II (e.g., Workstation, Printer OUs).

Note: Except where noted otherwise, the special permissions may include a wide range of permissions and properties and are acceptable for this requirement.

Note #2: The Special permissions for Authenticated Users are Read type. If detailed permissions include any Create, Delete, Modify, or Write Permissions or Properties is not in compliance with this recommendation.

Note #3: The Special permissions for Pre-Windows 2000 Compatible Access are for Read types. If detailed permissions include any Create, Delete, Modify, or Write Permissions or Properties is not in compliance with this recommendation.

Remediation:

Maintain the **Allow** type permissions on organization-defined OUs to be at least as restrictive as the defaults below.

- Open *Active Directory Users and Computers*
- Ensure *Advanced Features* is selected in the *View* menu

For each OU that is defined (folder in folder icon) excluding the Domain Controllers OU:

- Right-click the OU and select *Properties*
- Select the *Security* tab

Set the permission to the following: CREATOR OWNER - Special permissions, Self - Special permissions, Authenticated Users - Read, Special permissions, SYSTEM - Full Control, Domain Admins - Full Control, Enterprise Admins - Full Control, Key Admins - Special permissions, Enterprise Key Admins - Special permissions, Administrators - Read, Write, Create all child objects, Generate resultant set of policy (logging), Generate resultant set of policy (planning), Special permissions, Pre-Windows 2000 Compatible Access - Special permissions, and ENTERPRISE DOMAIN CONTROLLERS - Read, Special permissions

Note: The special permissions for Authenticated Users are Read type.

Note #2: The special permissions for Pre-Windows 2000 Compatible Access are for Read types.

Note #3: Document any additional permissions above Read with the ISSO if an approved distributed administration model (help desk or other user support staff) is implemented.

Default Value:

CREATOR OWNER - Special permissions, Self - Special permissions, Authenticated Users - Read, Special permissions, SYSTEM - Full Control, Domain Admins - Full Control, Enterprise Admins - Full Control, Key Admins - Special permissions, Enterprise Key Admins - Special permissions, Administrators - Read, Write, Create all child objects, Generate resultant set of policy (logging), Generate resultant set of policy (planning), Special permissions, Pre-Windows 2000 Compatible Access - Special permissions, and ENTERPRISE DOMAIN CONTROLLERS - Read, Special permissions

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224974
Rule ID: SV-224974r877392_rule
STIG ID: WN16-DC-000110
Severity: CAT I

20.44 Ensure 'Orphaned security identifiers (SIDs) must be removed from user rights' (Manual)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting ensures that orphaned security identifiers (SIDs) are removed from user rights.

Rationale:

Accounts or groups given rights on a system may show up as unresolved SIDs for various reasons including deletion of the accounts or groups. If the account or group objects are reanimated, there is a potential they may still have rights no longer intended. Valid domain accounts or groups may also show up as unresolved SIDs if a connection to the domain cannot be established for some reason.

Impact:

Orphaned security identifiers (SIDs) must be removed from user rights.

Audit:

Verify that orphaned security identifiers (SIDs) are not present in user rights assignment.

- Run *gpedit.msc*
- Navigate to *Local Computer Policy > Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights Assignment*

Review each User Right listed for any unresolved SIDs to determine whether they are valid, such as due to being temporarily disconnected from the domain. (Unresolved SIDs have the format that begins with "*S-1-".)

SID Groups

- S-1-5-11 - Authenticated Users
- S-1-5-113 - Local account
- S-1-5-114 - Local account and member of Administrators group
- S-1-5-19 - Local Service
- S-1-5-20 - Network Service
- S-1-5-32-544 - Administrators
- S-1-5-32-546 - Guests
- S-1-5-6 - Service
- S-1-5-9 - Enterprise Domain Controllers
- S-1-5-domain-512 - Domain Admins
- S-1-5-root domain-519 - Enterprise Admins
- S-1-5-80-3139157870-2983391045-3678747466-658725712-1809340420 - NT Service\WdiServiceHost

Remediation:

Remove any unresolved SIDs found in *User Rights assignments* for valid accounts or groups by removing the accounts or groups from the appropriate group policy.

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224863
Rule ID: SV-224863r569186_rule
STIG ID: WN16-00-000460
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.3 <u>Disable Dormant Accounts</u> Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.			
v7	16.8 <u>Disable Any Unassociated Accounts</u> Disable any account that cannot be associated with a business process or business owner.			

20.45 Ensure 'Outdated or unused accounts are removed or disabled' (Manual)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting ensures that all outdated or unused accounts are removed or disabled.

The recommended STIG state for this setting is: **35 days or older**.

Rationale:

Outdated or unused accounts provide penetration points that may go undetected. Inactive accounts must be deleted if no longer necessary or, if still required, disabled until needed.

Impact:

Outdated or unused accounts that are older than 35 days will be deleted or disabled.

Audit:

Verify that the system has no outdated or unused accounts 35 days and older:

Domain Controllers:

- Open *Windows PowerShell*
- Type *Search-ADAccount -AccountInactive -UsersOnly -TimeSpan 35.00:00:00*

This will return accounts that have not been logged on to for 35 days, along with various attributes such as the **Enabled** status and **LastLogonDate**.

Member servers and standalone systems:

- Open *Windows PowerShell*
- Type:

```
"([ADSI]('WinNT://{0}' -f $env:COMPUTERNAME)).Children | Where {
$_ .SchemaClassName -eq 'user' } | ForEach {
$user = ([ADSI]$_ .Path)
$lastLogin = $user.Properties.LastLogin.Value
$enabled = ($user.Properties.UserFlags.Value -band 0x2) -ne 0x2
if ($lastLogin -eq $null) {
$lastLogin = 'Never'
}
Write-Host $user.Name $lastLogin $enabled
}"
```

Note: You can copy or enter the lines above to the PowerShell window and hit enter. (Entering twice may be required. Do not include the quotes at the beginning and end of the query.)

This will return a list of local accounts with the account name, last logon, and if the account is enabled (True/False).

For example: User1 10/31/2015 5:49:56 AM True

Review the list of accounts returned by the above queries to determine the finding validity for each account reported.

Exclude the following accounts:

- Built-in administrator account (Renamed, SID ending in 500)
- Built-in guest account (Renamed, Disabled, SID ending in 501)
- Application accounts

Disable or delete any accounts 35 days or older.

Note: Inactive accounts that have been reviewed and deemed to be required must be documented with the Information System Security Officer (ISSO).

Remediation:

Regularly review accounts to determine if they are still active. Remove or disable accounts that have not been used in the last 35 days.

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224837
Rule ID: SV-224837r857230_rule
STIG ID: WN16-00-000210
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.3 <u>Disable Dormant Accounts</u> Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.			
v7	16.9 <u>Disable Dormant Accounts</u> Automatically disable dormant accounts after a set period of inactivity.			

20.46 Ensure 'Passwords are configured to expire' (Manual)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting ensures that all passwords for accounts are configured to expire.

Rationale:

Passwords that do not expire or are reused increase the exposure of a password with greater probability of being discovered or cracked.

Impact:

All passwords will be configured to expire.

Audit:

Verift that all passwords are configured to expire.

Domain Controllers:

- Open *PowerShell*
- Type *Search-ADAccount -PasswordNeverExpires -UsersOnly | FT Name, PasswordNeverExpires, Enabled*

Verify that all user accounts are **not** returned with **PasswordNeverExpires** with a status of *True*.

Note: Exclude application accounts, disabled accounts (e.g., DefaultAccount, Guest) and the krbtgt account.

Member servers and standalone systems:

- Open *PowerShell*
- Type *Get-CimInstance -Class Win32_Useraccount -Filter "PasswordExpires=False and LocalAccount=True" | FT Name, PasswordExpires, Disabled, LocalAccount*

Verify that all user accounts are **not** returned with **PasswordNeverExpires** with a status of *False*.

Note: Exclude application accounts and disabled accounts (e.g., DefaultAccount, Guest).

Remediation:

Configure all enabled user account passwords to expire.

Domain Controllers:

- Open *Active Directory Users and Computers*
- Uncheck **Password never expires** for all enabled user accounts

Member servers and standalone systems

- Open *Computer Management*
- Go to *Users*
- Uncheck **Password never expires** for all enabled user accounts

Note: Document any exceptions with the ISSO.

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224839
Rule ID: SV-224839r857235_rule
STIG ID: WN16-00-000230
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16.10 <u>Ensure All Accounts Have An Expiration Date</u> Ensure that all accounts have an expiration date that is monitored and enforced.			

20.47 Ensure 'Permissions for program file directories must conform to minimum requirements' (Manual)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting ensures that permissions for program file directories conform to minimum requirements.

The recommended STIG state for this setting is: `TrustedInstaller - Full control - This folder and subfolders, SYSTEM - Modify - This folder only, SYSTEM - Full control - Subfolders and files only, Administrators - Modify - This folder only, Administrators - Full control - Subfolders and files only, Users - Read & execute - This folder, subfolders and files, CREATOR OWNER - Full control - Subfolders and files only, ALL APPLICATION PACKAGES - Read & execute - This folder, subfolders, and files, and ALL RESTRICTED APPLICATION PACKAGES - Read & execute - This folder, subfolders, and files`

Rationale:

Changing the system's file and directory permissions allows the possibility of unauthorized and anonymous modification to the operating system and installed applications.

Impact:

Non-privileged groups such as Users or Authenticated Users must not have greater than "Read & execute" permissions except where noted as defaults. Individual accounts must not be used to assign permissions.

Audit:

Verify that program file directories (Program Files and Program Files [x86]) conform to minimum requirements:

Viewing in File Explorer:

- For each folder, view the Properties
- Select the *Security* tab
- Select the *Advanced* button

Default permissions:

\Program Files and \Program Files (x86)

Type - "Allow" for all

Inherited from - "None" for all

Principal - Access - Applies to

TrustedInstaller - Full control - This folder and subfolders, SYSTEM - Modify - This folder only, SYSTEM - Full control - Subfolders and files only, Administrators - Modify - This folder only, Administrators - Full control - Subfolders and files only, Users - Read & execute - This folder, subfolders and files, CREATOR OWNER - Full control - Subfolders and files only, ALL APPLICATION PACKAGES - Read & execute - This folder, subfolders, and files, and ALL RESTRICTED APPLICATION PACKAGES - Read & execute - This folder, subfolders, and files

Note: The default permissions are adequate when recommendation 2.3.10.5 *Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled'* is applied. (WN19-SO-000240).

OR

Verify with icacs:

- Open the *Command Prompt* as Administrator (Run as Admin)
- Type icacs followed by the directory:
 - `icacs "c:\program files"`
 - `icacs "c:\program files (x86)"`

The following results should be displayed:

```
c:\program files (c:\program files (x86))
NT SERVICE\TrustedInstaller:(F), NT
SERVICE\TrustedInstaller:(CI)(IO)(F). NT AUTHORITY\SYSTEM:(M), NT
AUTHORITY\SYSTEM:(OI)(CI)(IO)(F), BUILTIN\Administrators:(M),
BUILTIN\Administrators:(OI)(CI)(IO)(F), BUILTIN\Users:(RX),
BUILTIN\Users:(OI)(CI)(IO)(GR,GE), CREATOR OWNER:(OI)(CI)(IO)(F),
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(RX),
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION
PACKAGES:(OI)(CI)(IO)(GR,GE), APPLICATION PACKAGE AUTHORITY\ALL
RESTRICTED APPLICATION PACKAGES:(RX), and APPLICATION PACKAGE
AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(OI)(CI)(IO)(GR,GE)
```

Successfully processed 1 files; Failed processing 0 files

Remediation:

Maintain the default permissions for program file directories (Program Files and Program Files [x86]) and configure 2.3.10.5 *Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled'* (WN19-SO-000240).

Changing in File Explorer:

View the Properties of program file directories (Program Files and Program Files [x86]).

- For each folder, view the Properties
- Select the *Security* tab
- Select the *Advanced* button

TrustedInstaller - Full control - This folder and subfolders, SYSTEM - Modify - This folder only, SYSTEM - Full control - Subfolders and files only, Administrators - Modify - This folder only, Administrators - Full control - Subfolders and files only, Users - Read & execute - This folder, subfolders and files, CREATOR OWNER - Full control - Subfolders and files only, ALL APPLICATION PACKAGES - Read & execute - This folder, subfolders, and files, and ALL RESTRICTED APPLICATION PACKAGES - Read & execute - This folder, subfolders, and files

Default Value:

TrustedInstaller - Full control - This folder and subfolders, SYSTEM - Modify - This folder only, SYSTEM - Full control - Subfolders and files only, Administrators - Modify - This folder only, Administrators - Full control - Subfolders and files only, Users - Read & execute - This folder, subfolders and files, CREATOR OWNER - Full control - Subfolders and files only, ALL APPLICATION PACKAGES - Read & execute - This folder, subfolders, and files, and ALL RESTRICTED APPLICATION PACKAGES - Read & execute - This folder, subfolders, and files

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224833
Rule ID: SV-224833r852290_rule
STIG ID: WN16-00-000170
Severity: CAT II

20.48 Ensure 'Permissions for the Application Event Log must prevent access by non-privileged accounts' (Manual)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting restricts permissions to the Application Event Log for all non-privileged users.

The STIG recommended state for this setting is: **Eventlog - Full Control**, **SYSTEM - Full Control**, and **Administrators - Full Control**.

Rationale:

Restricting permissions on the Application Event Log will prevent non-privileged users from viewing and deleting the log. Preserving an audit trail of system activity can help identify possible compromises, detect attacks, and troubleshoot system performance and configuration errors.

Impact:

Non-privileged accounts will not be able to view or delete the Application Event Log.

Audit:

Navigate to the path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration, set the NTFS permissions on the file below to **Eventlog - Full Control**, **SYSTEM - Full Control**, and **Administrators - Full Control**:

```
%SystemRoot%\ System32\winevt\Logs\Application.evtx
```

Note: If the location of the event logs has been changed, when adding permissions, the event log user, **Eventlog** must be entered as **NT Service\Eventlog**.

Default Value:

Eventlog - Full Control; **SYSTEM - Full Control**; and **Administrators - Full Control**:

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224877
Rule ID: SV-224877r569186_rule
STIG ID: WN16-AU-000030
Severity: CAT II

20.49 Ensure 'Permissions for the Security Event Log must prevent access by non-privileged accounts' (Manual)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This setting restricts permissions to the Security Event Log for all non-privileged users.

The STIG recommended state for this setting is: **Eventlog - Full Control**, **SYSTEM - Full Control**, and **Administrators - Full Control**.

Rationale:

Restricting permissions on the Security Event Log will prevent non-privileged users from viewing and deleting the log. Preserving an audit trail of system activity can help identify possible compromises, detect attacks, and troubleshoot system performance and configuration errors.

Impact:

Non-privileged accounts will not be able to view or delete the Security Event Log.

Audit:

Navigate to the path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration, set the NTFS permissions on the file below to **Eventlog - Full Control**, **SYSTEM - Full Control**, and **Administrators - Full Control**:

```
%SystemRoot%\ System32\winevt\Logs\Security.evtx
```

Note: If the location of the event logs has been changed, when adding permissions, the event log user, **Eventlog** must be entered as **NT Service\Eventlog**.

Default Value:

Eventlog - Full Control; **SYSTEM - Full Control**; and **Administrators - Full Control**

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224878
Rule ID: SV-224878r569186_rule
STIG ID: WN16-AU-000040
Severity: CAT II

20.50 Ensure 'Permissions for the System Event Log must prevent access by non-privileged accounts' (Manual)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This setting restricts permissions to the System Event Log for all non-privileged users.

The STIG recommended state for this setting is: **Eventlog - Full Control**, **SYSTEM - Full Control**, and **Administrators - Full Control**.

Rationale:

Restricting permissions on the System Event Log will prevent non-privileged users from viewing and deleting the log. Preserving an audit trail of system activity can help identify possible compromises, detect attacks, and troubleshoot system performance and configuration errors.

Impact:

Non-privileged accounts will not be able to view or delete the System Event Log.

Audit:

Navigate to the path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration, set the NTFS permissions on the file below to **Eventlog - Full Control**, **SYSTEM - Full Control**, and **Administrators - Full Control**:

```
%SystemRoot%\ System32\winevt\Logs\System.evtx
```

Note: If the location of the event logs has been changed, when adding permissions, the event log user, **Eventlog** must be entered as **NT Service\Eventlog**.

Default Value:

Eventlog - Full Control; **SYSTEM - Full Control**; and **Administrators - Full Control**.

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224879
Rule ID: SV-224879r569186_rule
STIG ID: WN16-AU-000050
Severity: CAT II

20.51 Ensure 'Permissions for the system drive root directory must conform to minimum requirements' (Manual)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting ensures that the permissions for the system drive root directory (usually C:) conform to minimum requirements.

The recommended STIG state for this setting is: **SYSTEM - Full control - This folder, subfolders, and files, Administrators - Full control - This folder, subfolders, and files, Users - Read & execute - This folder, subfolders, and files, Users - Create folders/append data - This folder and subfolders, Users - Create files/write data - Subfolders only, and CREATOR OWNER - Full Control - Subfolders and files only**

Rationale:

Changing the system's file and directory permissions allows the possibility of unauthorized and anonymous modification to the operating system and installed applications.

Impact:

Non-privileged groups such as Users or Authenticated Users must not have greater than "Read & execute" permissions except where noted as defaults. Individual accounts must not be used to assign permissions.

Audit:

Verify that the system drive's root directory conforms to minimum requirements:

Viewing in File Explorer:

- View the Properties of the system drive's root directory (usually C:)
- Select the *Security* tab
- Select the *Advanced* button

Default permissions:

C:\

Type - "Allow" for all

Inherited from - "None" for all

Principal - Access - Applies to **SYSTEM - Full control - This folder, subfolders, and files, Administrators - Full control - This folder, subfolders, and files, Users - Read & execute - This folder, subfolders, and files, Users - Create folders/append data - This folder and subfolders, Users - Create files/write data - Subfolders only, and CREATOR OWNER - Full Control - Subfolders and files only**

Note: The default permissions are adequate when recommendation 2.3.10.5 *Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled'* is applied. (WN19-SO-000240).

OR

Verify with *icacls*:

- Open *Command Prompt* as Administrator (Run as Admin)
- Type *icacls* followed by the directory:
 - *icacls c:*

The following results should be displayed:

c:\

NT AUTHORITY\SYSTEM:(OI)(CI)(F), BUILTIN\Administrators:(OI)(CI)(F), BUILTIN\Users:(OI)(CI)(RX), BUILTIN\Users:(CI)(AD), BUILTIN\Users:(CI)(IO)(WD), and CREATOR OWNER:(OI)(CI)(IO)(F)

Successfully processed 1 files; Failed processing 0 files

Remediation:

Maintain the default permissions for the system drive's root directory and configure *2.3.10.5 Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled'* (WN19-SO-000240).

Changing in File Explorer:

- View the Properties of the system drive's root directory (usually C:)
- Select the *Security* tab
- Select the *Advanced* button

Change the permissions to match the default.

Default permissions:

C:

Type - "Allow" for all

Inherited from - "None" for all

Principal - Access - Applies to **SYSTEM** - Full control - This folder, subfolders, and files, **Administrators** - Full control - This folder, subfolders, and files, **Users** - Read & execute - This folder, subfolders, and files, **Users** - Create folders/append data - This folder and subfolders, **Users** - Create files/write data - Subfolders only, and **CREATOR OWNER** - Full Control - Subfolders and files only

Default Value:

Type - "Allow" for all

Inherited from - "None" for all

Principal - Access - Applies to **SYSTEM** - Full control - This folder, subfolders, and files, **Administrators** - Full control - This folder, subfolders, and files, **Users** - Read & execute - This folder, subfolders, and files, **Users** - Create folders/append data - This folder and subfolders, **Users** - Create files/write data - Subfolders only, and **CREATOR OWNER** - Full Control - Subfolders and files only

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224832
Rule ID: SV-224832r852289_rule
STIG ID: WN16-00-000160
Severity: CAT II

20.52 Ensure 'Permissions for the Windows installation directory conform to minimum requirements' (Manual)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting ensures permissions for the Windows installation directory conform to minimum requirements.

The recommended STIG state for this setting is: `TrustedInstaller - Full control - This folder and subfolders, SYSTEM - Modify - This folder only, SYSTEM - Full control - Subfolders and files only, Administrators - Modify - This folder only, Administrators - Full control - Subfolders and files only, Users - Read & execute - This folder, subfolders, and files, CREATOR OWNER - Full control - Subfolders and files only, ALL APPLICATION PACKAGES - Read & execute - This folder, subfolders, and files, and ALL RESTRICTED APPLICATION PACKAGES - Read & execute - This folder, subfolders, and files`

Rationale:

Changing the system's file and directory permissions allows the possibility of unauthorized and anonymous modification to the operating system and installed applications.

Impact:

Non-privileged groups such as Users or Authenticated Users must not have greater than "Read & execute" permissions except where noted as defaults. Individual accounts must not be used to assign permissions.

Audit:

Verify that the Windows installation directory conform to minimum requirements:

Viewing in File Explorer:

- For each folder, view the Properties
- Select the *Security* tab
- Select the *Advanced* button

Default permissions:

\Windows

Type - "Allow" for all

Inherited from - "None" for all

Principal - Access - Applies to

TrustedInstaller - Full control - This folder and subfolders, SYSTEM - Modify - This folder only, SYSTEM - Full control - Subfolders and files only, Administrators - Modify - This folder only, Administrators - Full control - Subfolders and files only, Users - Read & execute - This folder, subfolders, and files, CREATOR OWNER - Full control - Subfolders and files only, ALL APPLICATION PACKAGES - Read & execute - This folder, subfolders, and files, and ALL RESTRICTED APPLICATION PACKAGES - Read & execute - This folder, subfolders, and files

Note: Review the permissions for the Windows installation directory (usually C:\Windows). Non-privileged groups such as Users or Authenticated Users must not have greater than "Read & execute" permissions. Individual accounts must not be used to assign permissions.

Note #2: The default permissions are adequate when recommendation 2.3.10.5 *Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled'* is applied. (WN19-SO-000240).

OR

Verify with icaccls:

- Open the *Command Prompt* as Administrator (Run as Admin)
- Type icaccls followed by the directory:
 - icaccls c:\windows

The following results should be displayed:

c:\windows

NT SERVICE\TrustedInstaller:(F), NT
SERVICE\TrustedInstaller:(CI)(IO)(F), NT AUTHORITY\SYSTEM:(M), NT
AUTHORITY\SYSTEM:(OI)(CI)(IO)(F), BUILTIN\Administrators:(M),
BUILTIN\Administrators:(OI)(CI)(IO)(F), BUILTIN\Users:(RX),
BUILTIN\Users:(OI)(CI)(IO)(GR,GE), CREATOR OWNER:(OI)(CI)(IO)(F),
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(RX),
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION
PACKAGES:(OI)(CI)(IO)(GR,GE), APPLICATION PACKAGE AUTHORITY\ALL
RESTRICTED APPLICATION PACKAGES:(RX), and APPLICATION PACKAGE
AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(OI)(CI)(IO)(GR,GE)

Successfully processed 1 files; Failed processing 0 files

Remediation:

Maintain the default permissions for the Windows installation directory and configure
*2.3.10.5 Ensure 'Network access: Let Everyone permissions apply to anonymous users'
is set to 'Disabled' (WN19-SO-000240).*

- View the Properties of the Windows installation directory
- Select the *Security* tab
- Select the *Advanced* button

Change the permissions to match the default.

Default permissions:

\Windows

Type - "Allow" for all

Inherited from - "None" for all

Principal - Access - Applies to

TrustedInstaller - Full control - This folder and subfolders, SYSTEM -
Modify - This folder only, SYSTEM - Full control - Subfolders and files
only, Administrators - Modify - This folder only, Administrators - Full
control - Subfolders and files only, Users - Read & execute - This
folder, subfolders, and files, CREATOR OWNER - Full control -
Subfolders and files only, ALL APPLICATION PACKAGES - Read & execute -
This folder, subfolders, and files, and ALL RESTRICTED APPLICATION
PACKAGES - Read & execute - This folder, subfolders, and files

Default Value:

TrustedInstaller - Full control - This folder and subfolders, SYSTEM - Modify - This folder only, SYSTEM - Full control - Subfolders and files only, Administrators - Modify - This folder only, Administrators - Full control - Subfolders and files only, Users - Read & execute - This folder, subfolders, and files, CREATOR OWNER - Full control - Subfolders and files only, ALL APPLICATION PACKAGES - Read & execute - This folder, subfolders, and files, and ALL RESTRICTED APPLICATION PACKAGES - Read & execute - This folder, subfolders, and files

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224834
Rule ID: SV-224834r852291_rule
STIG ID: WN16-00-000180
Severity: CAT II

20.53 Ensure 'Permissions on Active Directory data files only allow System and Administrator access' (STIG DC only) (Manual)

Profile Applicability:

- STIG Domain Controller

Description:

This policy setting ensures that permissions on Active Directory data files only allow System and Administrator access.

Rationale:

Improper access permissions for directory data-related files could allow unauthorized users to read, modify, or delete directory data or audit trails.

Impact:

Users that do not have Administrator access will not be able to read, modify, or delete directory data or audit trails.

Audit:

Navigate to the following registry key and note the directory locations in the values for *Database log* files path and *DSA Database* file.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters
```

By default the location will be *\Windows\NTDS*.

If the locations are different, the following will need to be run for each location.

- Open the *Command Prompt* (Run as Administrator)
- Navigate to the NTDS directory (typically *\Windows\NTDS* by default)
- Type *icacls .*

If the permissions on each file are not as restrictive as the following it is not in compliance with this recommendation:

NT AUTHORITY\SYSTEM:(I)(F)

BUILTIN\Administrators:(I)(F)

(I) - permission inherited from parent container

(F) - full access

Remediation:

Change the permissions on the *NTDS database* and *log files* to the following:

NT AUTHORITY\SYSTEM:(I)(F)

BUILTIN\Administrators:(I)(F)

(I) - permission inherited from parent container

(F) - full access

Default Value:

\\Windows\\NTDS

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224970

Rule ID: SV-224970r877392_rule

STIG ID: WN16-DC-000070

Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

20.54 Ensure 'PKI certificates associated with user accounts must be issued by a DoD PKI or an approved External Certificate Authority (ECA)' (STIG DC only) (Manual)

Profile Applicability:

- STIG Domain Controller

Description:

This policy setting ensures that Public Key Infrastructure (PKI) certificates associated with user accounts are issued by DoD PKI or an approved External Certificate Authority (ECA).

Rationale:

Without proper issuance, certificates issued by an unauthorized Certificate Authority (CA) have limited value in authentication functions.

Impact:

None

Audit:

Verify that the PKI certificates associated with user accounts are issued by a DoD PKI or an approved External Certificate Authority (ECA):

- Open *PowerShell*
- Type *Get-ADUser -Filter * | FT Name, UserPrincipalName, Enabled*

If the User Principal Name (UPN) is not in the format of an individual's identifier for the certificate type and for the appropriate domain suffix, then this recommendation is not in compliance.

Note: Exclude disabled accounts (ex., DefaultAccount, Guest, and accounts).

Note #2: For standard NIPRNet certificates, the individual's identifier is in the format of an Electronic Data Interchange - Personnel Identifier (EDI-PI).

Note #3: Alternative Tokens and other certificates may use a different UPN format than the EDI-PI which vary by organization.

Remediation:

Map the user account to PKI certificates using the appropriate User Principal Name (UPN) for the network. See PKE documentation for details.

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224993
Rule ID: SV-224993r569186_rule
STIG ID: WN16-DC-000300
Severity: CAT I

20.55 Ensure 'Protection methods such as TLS, encrypted VPN's, or IPsec must be implemented if the data owner has a strict requirement for ensuring data integrity and confidentiality is maintained at every step of the data transfer and handling process' (Manual)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting ensures that protection methods such as TLS, encrypted VPNs, or IPsec are used if the data owner has a strict requirement for ensuring data integrity and confidentiality is maintained at every step of the data transfer and handling process.

Rationale:

Information can be either unintentionally or maliciously disclosed or modified during preparation for transmission, for example, during aggregation, at protocol transformation points, and during packing/unpacking. These unauthorized disclosures or modifications compromise the confidentiality or integrity of the information.

Ensuring the confidentiality of transmitted information requires the operating system to take measures in preparing information for transmission. This can be accomplished via access control and encryption.

Use of this requirement will be limited to situations where the data owner has a strict requirement for ensuring data integrity and confidentiality is maintained at every step of the data transfer and handling process. When transmitting data, operating systems need to support transmission protection mechanisms such as TLS, encrypted VPNs, or IPsec.

Impact:

Data integrity and confidentiality will need to be maintained at every step of the data transfer and handling process.

Audit:

If the data owner has a strict requirement for ensuring data integrity and confidentiality is maintained at every step of the data transfer and handling process, verify protection methods such as TLS, encrypted VPNs, or IPsec have been implemented.

Remediation:

Configure protection methods such as TLS, encrypted VPNs, or IPsec when the data owner has a strict requirement for ensuring data integrity and confidentiality is maintained at every step of the data transfer and handling process.

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224844
Rule ID: SV-224844r852298_rule
STIG ID: WN16-00-000290
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v8	3.11 <u>Encrypt Sensitive Data at Rest</u> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.			
v7	14.8 <u>Encrypt Sensitive Information at Rest</u> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			
v7	17.7 <u>Train Workforce on Sensitive Data Handling</u> Train workforce on how to identify and properly store, transfer, archive and destroy sensitive information.			

20.56 Ensure 'Separate NSA-approved (Type 1) cryptography is used' (STIG DC only) (Manual)

Profile Applicability:

- STIG Domain Controller

Description:

This policy setting ensures that separate NSA-approved (Type 1) cryptography is used to protect the directory data in transit for directory service implementations at a classified confidentiality level when replication data traverses a network cleared to a lower level than the data.

Rationale:

Directory data that is not appropriately encrypted is subject to compromise. Commercial-grade encryption does not provide adequate protection when the classification level of directory data in transit is higher than the level of the network.

Impact:

NSA approved cryptography and cryptographic equipment will be needed to comply with this recommendation.

Audit:

To ensure that separate NSA-approved (Type 1) cryptography is used, perform the following:

- Review the organization network diagram(s) or documentation to determine the level of classification for the network(s) over which replication data is transmitted.
- Determine the classification level of the Windows domain controller.

If the classification level of the Windows domain controller is higher than the level of the networks, review the organization network diagram(s) and directory implementation documentation to determine if NSA-approved encryption is used to protect the replication network traffic.

If the classification level of the Windows domain controller is higher than the level of the network traversed and NSA-approved encryption is not used, this is not in compliance.

Remediation:

Configure a NSA-approved (Type 1) cryptography to protect the directory data in transit for directory service implementations at a classified confidentiality level that transfer replication data through a network cleared to a lower level than the data.

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224977
Rule ID: SV-224977r878117_rule
STIG ID: WN16-DC-000140
Severity: CAT II

20.57 Ensure 'Server Message Block (SMB) v1 protocol must not be installed' (Manual)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting ensures that Server Message Block (SMB) v1 protocol is not installed on the system. SMBv1 is a legacy version of the Server Message Block protocol Windows uses for file sharing on a local network.

The STIG recommended state for this setting is: **Not installed**.

Rationale:

SMBv1 is a legacy protocol that uses the MD5 algorithm as part of SMB. MD5 is known to be vulnerable to a number of attacks such as collision and preimage attacks and is not FIPS compliant.

Impact:

Disabling SMBv1 without thoroughly testing for SMBv1 traffic in your environment can have unintended consequences, up to and including a complete suspension of all network services, denied access to all resources, and remote authentication failures (like LDAP).

Audit:

Navigate to the path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To uninstall the *SMBv1 protocol*:

- Start *Server Manager*
- Select the *server* with the role
- Scroll down to *ROLES AND FEATURES* in the right pane
- Select *Remove Roles and Features* from the drop-down *TASKS* list
- Select the appropriate server on the *Server Selection* page and click *Next*
- Deselect *SMB 1.0/CIFS File Sharing Support* on the *Features* page
- Click next and *Remove* as prompted (if installed).

OR

- Open *Windows PowerShell* with elevated privileges (run as administrator)
- Type *Uninstall-WindowsFeature -Name FS-SMB1 -Restart* (Omit the *Restart* parameter if an immediate restart of the system cannot be done.)

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224856
Rule ID: SV-224856r569186_rule
STIG ID: WN16-00-000410
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			
v7	<u>14.3 Disable Workstation to Workstation Communication</u> Disable all workstation to workstation communication to limit an attacker's ability to move laterally and compromise neighboring systems, through technologies such as Private VLANs or microsegmentation.			

20.58 Ensure 'Shared user accounts do not exist' (Manual)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting ensures that shared user accounts do not exist.

Note: Shared accounts, such as required by an application, may be approved by the organization. This must be documented with the ISSO. Documentation must include the reason for the account, who has access to the account, and how the risk of using the shared account is mitigated to include monitoring account activity.

Rationale:

Shared accounts (accounts where two or more people log on with the same user identification) do not provide adequate identification and authentication. There is no way to provide for nonrepudiation or individual accountability for system access and resource usage.

Impact:

Shared users accounts will not be permitted within the organization.

Audit:

Determine whether any shared accounts exist.

Remediation:

Remove unapproved shared accounts from the system.

Note: Shared accounts, such as required by an application, may be approved by the organization. This must be documented with the ISSO. Documentation must include the reason for the account, who has access to the account, and how the risk of using the shared account is mitigated to include monitoring account activity.

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224825
Rule ID: SV-224825r569186_rule
STIG ID: WN16-00-000080
Severity: CAT II

20.59 Ensure 'Software certificate installation files must be removed' (Manual)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting ensures that unauthorized certificate installation files (*.p12 and *.pfx) are not installed on the system. *.p12 and *.pfx files are a binary format used for storing the server certificate, any intermediate certificates, and the private key into a single encryptable file.

The STIG recommended state for this setting is: Remove all *.p12 and *.pfx files.

Note: This does not apply to server-based applications that have a requirement for .p12 certificate files or Adobe PreFlight certificate files.

Rationale:

Use of software certificates and their accompanying installation files for end users to access resources is less secure than the use of hardware-based certificates.

Impact:

*.p12 and *.pfx will not be allowed on the system.

Note: This does not apply to server-based applications that have a requirement for .p12 certificate files or Adobe PreFlight certificate files. Some applications create files with extensions of .p12 that are not certificate installation files. Removal of non-certificate installation files from systems is not required. These must be documented with the ISSO.

Audit:

Navigate to the path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

Remove any certificate installation files ***.p12** and ***.pfx** found on a system.

Note: The Certificate Store can be loaded by executing the *Microsoft Management Console (MMC)* and loading the *Certificates* snap-in.

Note #2: This does not apply to server-based applications that have a requirement for .p12 certificate files or Adobe PreFlight certificate files. Some applications create files with extensions of .p12 that are not certificate installation files. Removal of non-certificate installation files from systems is not required. These must be documented with the ISSO.

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224842
Rule ID: SV-224842r569186_rule
STIG ID: WN16-00-000270
Severity: CAT II

20.60 Ensure 'System files must be monitored for unauthorized changes' (Manual)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting ensures that system files are monitored for unauthorized changes.

Rationale:

Monitoring system files for changes against a baseline on a regular basis may help detect the possible introduction of malicious code on a system.

Impact:

Monitoring system files for changes against a baseline on a regular basis will be required.

Audit:

Verify that the system is monitored for unauthorized changes to system files (e.g., *.exe, *.bat, *.com, *.cmd, and *.dll) against a baseline on a weekly basis.

Note: A properly configured and approved DoD HBSS solution that supports a File Integrity Monitor (FIM) module will meet the requirement for file integrity checking.

Remediation:

Monitor the system for unauthorized changes to system files (e.g., *.exe, *.bat, *.com, *.cmd, and *.dll) against a baseline on a weekly basis. This can be done with the use of various monitoring tools including the approved DoD HBSS solution that supports a File Integrity Monitor (FIM) module.

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224840
Rule ID: SV-224840r891691_rule
STIG ID: WN16-00-000240
Severity: CAT II

20.61 Ensure 'Systems requiring data at rest protections must employ cryptographic mechanisms to prevent unauthorized disclosure and modification of the information at rest' (Manual)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting ensures that systems requiring data at rest protections must employ cryptographic mechanisms to prevent unauthorized disclosure and modification of the information at rest.

Rationale:

Encrypting data at rest protects the organization from the physical theft of the file system storage devices. It can also protect the organization from unauthorized access to computer data.

Impact:

Selection of a cryptographic mechanism is based on the need to protect the integrity of organizational information. The strength of the mechanism is commensurate with the security category and/or classification of the information. Organizations have the flexibility to either encrypt all information on storage devices (i.e., full disk encryption) or encrypt specific data structures (e.g., files, records, or fields).

Audit:

Verify systems that require additional protections due to factors such as inadequate physical protection or sensitivity of the data employ encryption to protect the confidentiality and integrity of all information at rest.

Remediation:

Configure systems that require additional protections due to factors such as inadequate physical protection or sensitivity of the data to employ encryption to protect the confidentiality and integrity of all information at rest.

Note: This requirement addresses protection of user-generated data as well as operating system-specific configuration data. Organizations may choose to employ different mechanisms to achieve confidentiality and integrity protections, as appropriate, in accordance with the security category and/or classification of the information.

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224843
Rule ID: SV-224843r953813_rule
STIG ID: WN16-00-000280
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 <u>Encrypt Sensitive Data at Rest</u> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	14.8 <u>Encrypt Sensitive Information at Rest</u> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			●

20.62 Ensure 'Telnet Client is not installed' (Manual)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting enables a remote user to log on to this computer and run programs, and supports various TCP/IP Telnet clients, including UNIX-based and Windows-based computers.

The STIG recommended state for this setting is: **Not Installed**.

Note: This service is not installed by default. It is supplied with Windows but is installed by enabling an optional Windows feature (_Telnet Client).

Rationale:

Hosting a Telnet server (especially a non-secure Telnet) from a workstation is an increased security risk, as the attack surface of that workstation is then greatly increased.

Note: This security concern applies to any Telnet application installed on a workstation, not just the one supplied with Windows.

Impact:

Remote user Telnet access will not be available.

Audit:

To establish the recommended configuration, navigate to the the following and ensure that the Telnet Client feature is **Not installed**:

- Run *PowerShell*
- Type *Get-WindowsFeature | Where Name -eq Telnet-Client*
If *Installed State* is **Installed** this is not in compliance with the recommendation.

Note: An *Installed State* of **Available** or **Removed** is in compliance with the recommendation.

Note #2: Alternately this Windows Feature can be uninstalled by using Roles and Features in Server Manager.

Remediation:

To establish the recommended configuration, navigate to the following and **Uninstall** the Telnet Client feature:

To Uninstall the Telnet Client feature:

- Start *Server Manager*
- Select the server with the role
- Scroll down to *ROLES AND FEATURES* in the right pane
- Select *Remove Roles and Features* from the drop-down *TASKS* list
- Select the appropriate server on the *Server Selection* page and click *Next*
- Deselect *Telnet Client* on the *Features* page
- Click *Next* and *Remove* as prompted (if installed).

Default Value:

Not installed

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224854
Rule ID: SV-224854r569186_rule
STIG ID: WN16-00-000390
Severity: CAT II

20.63 Ensure 'Temporary user accounts must be automatically removed or disabled after 72 hours' (Manual)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting ensures that temporary user accounts are automatically removed or disabled after the crisis is resolved or within 72 hours of the crisis.

Temporary accounts are established as part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation.

Rationale:

If temporary user accounts remain active when no longer needed or for an excessive period, these accounts may be used to gain unauthorized access. To mitigate this risk, automated termination of all temporary accounts must be set upon account creation.

To address access requirements, many operating systems may be integrated with enterprise-level authentication/access mechanisms that meet or exceed access control policy requirements.

Impact:

If temporary accounts are used, the operating system must be configured to automatically terminate these types of accounts after a DoD-defined time period of 72 hours.

Audit:

Verify if temporary user accounts are used and identify any that exist:

Domain Controller:

- Open *PowerShell*
- Type *Search-ADAccount -AccountExpiring | FT Name, AccountExpirationDate*

If **AccountExpirationDate** has been defined and is not within 72 hours for an emergency administrator account, this is a finding.

Member servers/Stand-alone systems:

- Open the *Command Prompt*
- Type *Net user [username]* where [username] is the name of the emergency account.

If **Account expires** has been defined and is not within 72 hours for an emergency administrator account, this is a finding.

If temporary user cannot be configured with an expiration date due to an ongoing crisis, the accounts must be disabled or removed when the crisis is resolved.

If temporary user accounts have not been configured with an expiration date or have not been disabled or removed following the resolution of a crisis, this is a finding.

Remediation:

Remove any temporary user accounts after a crisis has been resolved or configure the accounts to automatically expire within 72 hours.

Domain accounts can be configured with an account expiration date, under *Account* properties.

Local accounts can be configured to expire with the following command:

- Open the *Command Prompt*
- Type *Net user [username] /expires:[mm/dd/yyyy]* where username is the name of the temporary user account

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224848
Rule ID: SV-224848r857240_rule
STIG ID: WN16-00-000330
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16.8 <u>Disable Any Unassociated Accounts</u> Disable any account that cannot be associated with a business process or business owner.			

20.64 Ensure 'TFTP Client' is 'not installed' (Manual)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This setting provides the transfer of files to and from a remote computer, typically a computer running UNIX, that is running the Trivial File Transfer Protocol (tftp) service or daemon. tftp is typically used by embedded devices or systems that retrieve firmware, configuration information, or a system image during the boot process from a tftp server.

The STIG recommended state for this setting is: **Not installed**.

Rationale:

Unnecessary services increase the attack surface of a system. Some of these services may not support required levels of authentication or encryption or may provide unauthorized access to the system.

Impact:

Trivial File Transfer Protocol (tftp) features, such as the transferring of files, will not be available to users in your organization.

Audit:

Navigate to the path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To Uninstall the *TFTP Client* feature:

- Start "Server Manager"
- Select the server with the role
- Scroll down to "ROLES AND FEATURES" in the right pane
- Select "Remove Roles and Features" from the drop-down "TASKS" list
- Select the appropriate server on the "Server Selection" page and click "Next"
- Deselect "TFTP Client" on the "Features" page
- Click "Next" and "Remove" as prompted (if installed).

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224855
Rule ID: SV-224855r569186_rule
STIG ID: WN16-00-000400
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

20.65 Ensure 'The system must have the Roles and Features required for it documented' (Manual)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting ensures that Roles and Features required by the system are documented.

Rationale:

Unnecessary Roles and Features increase the attack surface of a system. Limiting roles and features of a system to only those necessary reduces this potential. The standard installation option (previously called Server Core) further reduces this when selected at installation.

Impact:

Roles and Features must be documented.

Audit:

Verify that only necessary roles and features are installed on the system.

- Open PowerShell
- Run *Get-WindowsFeature*
- Review the roles and features with an *Install State* and determine if they are necessary on the system

Note: Required roles and features will vary based on the function of the individual system.

Note #2: Roles and features specifically required to be disabled per the STIG are identified in separate requirements.

Remediation:

Document the roles and features required for the system to operate. Uninstall roles and features that are not required.

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224845
Rule ID: SV-224845r569186_rule
STIG ID: WN16-00-000300
Severity: CAT II

20.66 Ensure 'The system uses a host-based intrusion detection or prevention system' (Manual)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting ensures that the operating system (OS) has a host-based intrusion detection (HIDS) or prevention system (HIPS) installed.

Rationale:

A properly configured Host-based Intrusion Detection System (HIDS) or Host-based Intrusion Prevention System (HIPS) provides another level of defense against unauthorized access to critical servers. With proper configuration and logging enabled, such a system can stop and/or alert for attempts to gain unauthorized access to resources.

Impact:

A host-based intrusion detection (HIDS) or prevention system (HIPS) must be installed on the system.

Audit:

Determine whether there is a HIDS or HIPS on each server.

If the HIPS component of HBSS is installed and active on the host and the alerts of blocked activity are being logged and monitored, this meets the requirement.

A HIDS device is not required on a system that has the role as the Network Intrusion Device (NID). However, this exception needs to be documented with the ISSO.

Remediation:

Install a HIDS or HIPS on each server.

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224830
Rule ID: SV-224830r793223_rule
STIG ID: WN16-00-000140
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.6 <u>Centrally Manage Anti-Malware Software</u> Centrally manage anti-malware software.		●	●
v7	8.1 <u>Utilize Centrally Managed Anti-malware Software</u> Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

20.67 Ensure 'The system uses an anti-virus program' (Manual)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting ensures that the system uses an anti-virus program.

Rationale:

Malicious software can establish a base on individual desktops and servers. Employing an automated mechanism to detect this type of software will aid in elimination of the software from the operating system.

Impact:

Anti-virus software must be installed on the system and if not configured correctly may prohibit the user of Features and Programs.

Audit:

Verify an anti-virus solution is installed on the system. The anti-virus solution may be bundled with an approved host-based security solution.

To verify if Windows Defender is in use:

- Open *PowerShell*
- Type *get-service | where {\$_.DisplayName -Like "Defender"} | Select Status,DisplayName_*

To verify if third-party anti-virus is in use or enabled:

- Open *PowerShell*
- Type *get-service | where {\$_.DisplayName -Like "mcafee"} | Select Status,DisplayName_*, type *get-service | where {\$_.DisplayName -Like "symantec"} | Select Status,DisplayName_*

Remediation:

If no anti-virus software is in use, install Windows Defender or third-party anti-virus.

- Open *PowerShell*
- Type *Install-WindowsFeature -Name Windows-Defender*

For third-party anti-virus, install per anti-virus instructions and disable Windows Defender.

- Open *PowerShell*
- Type *Uninstall-WindowsFeature -Name Windows-Defender*

Default Value:

Windows defender - Enabled

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224829
Rule ID: SV-224829r569237_rule
STIG ID: WN16-00-000120
Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.6 <u>Centrally Manage Anti-Malware Software</u> Centrally manage anti-malware software.		●	●
v7	8.1 <u>Utilize Centrally Managed Anti-malware Software</u> Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

20.68 Ensure 'Unified Extensible Firmware Interface (UEFI) firmware must be configured and run in UEFI mode, not Legacy BIOS' (Manual)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting ensures that systems have Unified Extensible Firmware Interface (UEFI) firmware and is configured to run in UEFI mode, and not Legacy BIOS mode.

The STIG recommended state for this setting is: **UEFI mode**.

Rationale:

UEFI provides additional security features in comparison to legacy BIOS firmware, including Secure Boot. UEFI is required to support additional security features in Windows, including Virtualization Based Security and Credential Guard.

Impact:

Systems with UEFI that are operating in Legacy BIOS mode will not support Virtualization Based Security and Credential Guard.

Audit:

To verify the system firmware is configured to run in *UEFI* mode, not *Legacy BIOS*:

- Run *System Information*
- Go to *System Summary*
- Ensure *BIOS Mode* displays *UEFI*

Note: Some older systems may not have UEFI firmware. This is currently a CAT III; it will be raised in severity at a future date when broad support of Windows hardware and firmware requirements are expected to be met. Devices that have UEFI firmware must run in **UEFI** mode.

Remediation:

To enable UEFI firmware to run in **UEFI** mode, not *Legacy BIOS* mode.

- Open the PC BIOS menu. This menu can usually be accessed by pressing a key during the bootup sequence, such as F1, F2, F12, or Esc
- OR from Windows, hold the Shift key while selecting Restart. Go to Troubleshoot > Advanced Options: UEFI Firmware Settings
- Find the *Boot Device Menu* select the command that identifies both the firmware mode and the device
- Select *UEFI* mode
- Save changes and exit. The PC will reboot

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224865
Rule ID: SV-224865r569186_rule
STIG ID: WN16-00-000480
Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 <u>Enable Anti-Exploitation Features</u> Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.			

20.69 Ensure 'US DoD CCEB Interoperability Root CA cross-certificates' are installed in the 'Untrusted Certificates Store' on unclassified systems (Manual)

Profile Applicability:

- STIG Member Server
- STIG Domain Controller

Description:

This policy setting ensures that the US DoD Combined Communications-Electronics Board (CCEB) Interoperability Root CA cross-certificates are installed in the Untrusted Certificate Store on unclassified systems.

The STIG recommended state for this setting is: **DoD Root CA 3 - US DoD CCEB Interoperability Root CA 2 - 9B74964506C7ED9138070D08D5F8B969866560C8**.

Rationale:

If the Interoperability Root CA cross-certificates are not installed in the Untrusted Certificates Store users may experience denial of service when performing certificate-based authentication to DoD websites due to the system chaining to a root other than DoD Root CAs.

Note: This requirement only applies to unclassified systems.

Impact:

N/A

Audit:

To establish the recommended configuration, navigate to the *Untrusted Certificate Store* to ensure the following certificates are installed:

DoD Root CA 3 - US DoD CCEB Interoperability Root CA 2 - 9B74964506C7ED9138070D08D5F8B969866560C8

Note: The Certificate Store can be loaded by executing the *Microsoft Management Console (MMC)* and loading the *Certificates* snap-in.

Remediation:

Install the following DoD Root CA certificates in the *Untrusted Certificates Store*:

DoD Root CA 3 - US DoD CCEB Interoperability Root CA 2 -
9B74964506C7ED9138070D08D5F8B969866560C8.

Note: The InstallRoot tool is available on IASE at <http://iase.disa.mil/pki-pke/Pages/tools.aspx>.

Note #2: The Certificate Store can be loaded by executing the *Microsoft Management Console (MMC)* and loading the *Certificates* snap-in.

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2019 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-225023
Rule ID: SV-225023r890514_rule
STIG ID: WN16-PK-000030
Severity: CAT II

20.70 Ensure 'Users with Administrative privileges have separate accounts for administrative duties and normal operational tasks' (Manual)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

This policy setting ensures that users with administrative privileges must have separate accounts for administrative duties and normal user tasks.

Rationale:

Allowing a user with administrative privileges to perform normal user tasks such as checking email or accessing the Internet is a security risk. If an attacker gains control of administrative privileges, this makes the computer and network vulnerable to malicious software due to having full administrative privileges.

Impact:

A user with administrative privileges will have two accounts, one for normal user tasks and one for administrative duties.

Audit:

Ensure each user with administrative privileges has been assigned a unique administrative account separate from their standard user account. This can be achieved by checking the user's account in *Active Directory Users and Computers*.

Remediation:

If a standard user account is found to have administrative privileges, remove the privileges from the standard user account, and create an administrative account for the user.

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224819
Rule ID: SV-224819r569186_rule
STIG ID: WN16-00-000010
Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</u> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.			
v7	<u>4.3 Ensure the Use of Dedicated Administrative Accounts</u> Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.			

20.71 Ensure 'Windows PowerShell 2.0' is 'not installed' (Manual)

Profile Applicability:

- STIG Domain Controller
- STIG Member Server

Description:

Windows PowerShell was designed with the purpose of task automation and configuration management.

The STIG recommended state for this setting is: **Not installed**.

Rationale:

Windows PowerShell 2.0 can be used in some scenarios by attackers who want to bypass the script block logging feature that was added in PowerShell 5.0.7.

Impact:

PowerShell scripts that rely on PowerShell 2.0 will not function in your environment.

Audit:

Navigate to the path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To Uninstall the *Windows PowerShell 2.0 Engine* feature:

- Open *Server Manager*
- Select the *server* with the role
- Scroll down to *ROLES AND FEATURES* in the right pane
- Select *Remove Roles and Features* from the drop-down *TASKS* list
- Select the appropriate server on the *Server Selection* page and click next
- Deselect *Windows PowerShell 2.0 Engine* under *Windows PowerShell* on the *Features* page
- Click next and *Remove* as prompted (if installed)

Note: Windows PowerShell 5.0 added advanced logging features that can provide additional detail when malware has been run on a system.

Default Value:

N/A

Additional Information:

Microsoft Windows Server 2016 Security Technical Implementation Guide:
Version 2, Release 8, Benchmark Date: May 15, 2024

Vul ID: V-224859
Rule ID: SV-224859r569186_rule
STIG ID: WN16-00-000420
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.3 <u>Address Unauthorized Software</u> Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.			
v7	2.6 <u>Address unapproved software</u> Ensure that unauthorized software is either removed or the inventory is updated in a timely manner			

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	Account Policies		
1.1	Password Policy		
1.1.1	Ensure 'Enforce password history' is set to '24 or more password(s)' (Automated)	☐	☐
1.1.2	Ensure 'Maximum password age' is set to '365 or fewer days, but not 0' (Automated)	☐	☐
1.1.3	Ensure 'Maximum password age' is set to '60 or fewer days, but not 0' (STIG only) (Automated)	☐	☐
1.1.4	Ensure 'Minimum password age' is set to '1 or more day(s)' (Automated)	☐	☐
1.1.5	Ensure 'Minimum password length' is set to '14 or more character(s)' (Automated)	☐	☐
1.1.6	Ensure 'Password must meet complexity requirements' is set to 'Enabled' (Automated)	☐	☐
1.1.7	Ensure 'Store passwords using reversible encryption' is set to 'Disabled' (Automated)	☐	☐
1.2	Account Lockout Policy		
1.2.1	Ensure 'Account lockout duration' is set to '15 or more minute(s)' (Automated)	☐	☐
1.2.2	Ensure 'Account lockout threshold' is set to '5 or fewer invalid logon attempt(s), but not 0' (Automated)	☐	☐
1.2.3	Ensure 'Account lockout threshold' is set to '3 or fewer invalid logon attempt(s), but not 0' (STIG only) (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.2.4	Ensure 'Allow Administrator account lockout' is set to 'Enabled' (MS only) (Manual)	☐	☐
1.2.5	Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)' (Automated)	☐	☐
1.3	Kerberos Policy		
1.3.1	Ensure 'Enforce user logon restrictions' is set to 'Enabled' (STIG DC only) (Manual)	☐	☐
1.3.2	Ensure 'Maximum lifetime for service ticket' is set to '600 or fewer minutes, but not 0' (STIG DC only) (Manual)	☐	☐
1.3.3	Ensure 'Maximum lifetime for user ticket' is set to '10 or fewer hours, but not 0' (STIG DC only) (Manual)	☐	☐
1.3.4	Ensure 'Maximum lifetime for user ticket renewal' is set to '7 or fewer days' (STIG DC only) (Manual)	☐	☐
1.3.5	Ensure 'Maximum tolerance for computer clock synchronization' is set to '5 or fewer minutes' (STIG DC only) (Manual)	☐	☐
2	Local Policies		
2.1	Audit Policy		
2.2	User Rights Assignment		
2.2.1	Ensure 'Access Credential Manager as a trusted caller' is set to 'No One' (Automated)	☐	☐
2.2.2	Ensure 'Access this computer from the network' is set to 'Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS' (DC only) (Automated)	☐	☐
2.2.3	Ensure 'Access this computer from the network' is set to 'Administrators, Authenticated Users' (MS only) (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.2.4	Ensure 'Act as part of the operating system' is set to 'No One' (Automated)	☐	☐
2.2.5	Ensure 'Add workstations to domain' is set to 'Administrators' (DC only) (Automated)	☐	☐
2.2.6	Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE' (Automated)	☐	☐
2.2.7	Ensure 'Allow log on locally' is set to 'Administrators, ENTERPRISE DOMAIN CONTROLLERS' (DC only) (Automated)	☐	☐
2.2.8	Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators' (DC only) (Automated)	☐	☐
2.2.9	Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators, Remote Desktop Users' (MS only) (Automated)	☐	☐
2.2.10	Ensure 'Back up files and directories' is set to 'Administrators' (Automated)	☐	☐
2.2.11	Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE' (Automated)	☐	☐
2.2.12	Ensure 'Change the time zone' is set to 'Administrators, LOCAL SERVICE' (Automated)	☐	☐
2.2.13	Ensure 'Create a pagefile' is set to 'Administrators' (Automated)	☐	☐
2.2.14	Ensure 'Create a token object' is set to 'No One' (Automated)	☐	☐
2.2.15	Ensure 'Create global objects' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (Automated)	☐	☐
2.2.16	Ensure 'Create permanent shared objects' is set to 'No One' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.2.17	Ensure 'Create symbolic links' is set to 'Administrators' (DC only) (Automated)	☐	☐
2.2.18	Ensure 'Create symbolic links' is set to 'Administrators, NT VIRTUAL MACHINE\Virtual Machines' (MS only) (Automated)	☐	☐
2.2.19	Ensure 'Debug programs' is set to 'Administrators' (Automated)	☐	☐
2.2.20	Ensure 'Deny access to this computer from the network' to include 'Guests' (DC only) (Automated)	☐	☐
2.2.21	Ensure 'Deny access to this computer from the network' to include 'Guests, Local account and member of Administrators group' (MS only) (Automated)	☐	☐
2.2.22	Ensure 'Deny access to this computer from the network' to include 'Guests, Enterprise Admins Group, Domains Admins Group, Local account, and member of Administrators group' (STIG MS only) (Automated)	☐	☐
2.2.23	Ensure 'Deny log on as a batch job' to include 'Guests' (Automated)	☐	☐
2.2.24	Ensure 'Deny log on as a batch job' to include 'Guests, Enterprise Admins Group, and Domain Admins Group' (STIG MS only) (Automated)	☐	☐
2.2.25	Ensure 'Deny log on as a service' to include 'Guests' (Automated)	☐	☐
2.2.26	Ensure 'Deny log on as a service' to include 'No one' (STIG DC only) (Automated)	☐	☐
2.2.27	Ensure 'Deny log on as a service' to include 'Enterprise Admins Group and Domain Admins Group' (STIG MS only) (Automated)	☐	☐
2.2.28	Ensure 'Deny log on locally' to include 'Guests' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.2.29	Ensure 'Deny log on locally' to include 'Guests, Enterprise Admins group, and Domain Admins group' (STIG MS only) (Automated)	☐	☐
2.2.30	Ensure 'Deny log on through Remote Desktop Services' to include 'Guests' (DC only) (Automated)	☐	☐
2.2.31	Ensure 'Deny log on through Remote Desktop Services' is set to 'Guests, Local account' (MS only) (Automated)	☐	☐
2.2.32	Ensure 'Deny log on through Remote Desktop Services' is set to 'Guests, Local account, Enterprise Admins Group, and Domain Admins Group' (STIG MS only) (Automated)	☐	☐
2.2.33	Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'Administrators' (DC only) (Automated)	☐	☐
2.2.34	Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'No One' (MS only) (Automated)	☐	☐
2.2.35	Ensure 'Force shutdown from a remote system' is set to 'Administrators' (Automated)	☐	☐
2.2.36	Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE' (Automated)	☐	☐
2.2.37	Ensure 'Impersonate a client after authentication' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (DC only) (Automated)	☐	☐
2.2.38	Ensure 'Impersonate a client after authentication' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' and (when the Web Server (IIS) Role with Web Services Role Service is installed) 'IIS_IUSRS' (MS only) (Automated)	☐	☐
2.2.39	Ensure 'Impersonate a client after authentication' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (STIG MS only) (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.2.40	Ensure 'Increase scheduling priority' is set to 'Administrators' (Automated)	☐	☐
2.2.41	Ensure 'Load and unload device drivers' is set to 'Administrators' (Automated)	☐	☐
2.2.42	Ensure 'Lock pages in memory' is set to 'No One' (Automated)	☐	☐
2.2.43	Ensure 'Log on as a batch job' is set to 'Administrators' (DC Only) (Automated)	☐	☐
2.2.44	Ensure 'Manage auditing and security log' is set to 'Administrators' (DC only) (Automated)	☐	☐
2.2.45	Ensure 'Manage auditing and security log' is set to 'Administrators' (MS only) (Automated)	☐	☐
2.2.46	Ensure 'Manage auditing and security log' is set to 'Administrators' (STIG DC only) (Automated)	☐	☐
2.2.47	Ensure 'Modify an object label' is set to 'No One' (Automated)	☐	☐
2.2.48	Ensure 'Modify firmware environment values' is set to 'Administrators' (Automated)	☐	☐
2.2.49	Ensure 'Perform volume maintenance tasks' is set to 'Administrators' (Automated)	☐	☐
2.2.50	Ensure 'Profile single process' is set to 'Administrators' (Automated)	☐	☐
2.2.51	Ensure 'Profile system performance' is set to 'Administrators, NT SERVICE\WdiServiceHost' (Automated)	☐	☐
2.2.52	Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE' (Automated)	☐	☐
2.2.53	Ensure 'Restore files and directories' is set to 'Administrators' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.2.54	Ensure 'Shut down the system' is set to 'Administrators' (Automated)	☐	☐
2.2.55	Ensure 'Synchronize directory service data' is set to 'No One' (DC only) (Automated)	☐	☐
2.2.56	Ensure 'Take ownership of files or other objects' is set to 'Administrators' (Automated)	☐	☐
2.3	Security Options		
2.3.1	Accounts		
2.3.1.1	Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts' (Automated)	☐	☐
2.3.1.2	Ensure 'Accounts: Guest account status' is set to 'Disabled' (MS only) (Automated)	☐	☐
2.3.1.3	Ensure 'Accounts: Guest account status' is set to 'Disabled' (STIG only) (Automated)	☐	☐
2.3.1.4	Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled' (Automated)	☐	☐
2.3.1.5	Configure 'Accounts: Rename administrator account' (Automated)	☐	☐
2.3.1.6	Configure 'Accounts: Rename guest account' (Automated)	☐	☐
2.3.2	Audit		
2.3.2.1	Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled' (Automated)	☐	☐
2.3.2.2	Ensure 'Audit: Shut down system immediately if unable to log security audits' is set to 'Disabled' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.3	DCOM		
2.3.4	Devices		
2.3.4.1	Ensure 'Devices: Prevent users from installing printer drivers' is set to 'Enabled' (Automated)	☐	☐
2.3.5	Domain controller		
2.3.5.1	Ensure 'Domain controller: Allow server operators to schedule tasks' is set to 'Disabled' (DC only) (Automated)	☐	☐
2.3.5.2	Ensure 'Domain controller: Allow vulnerable Netlogon secure channel connections' is set to 'Not Configured' (DC Only) (Automated)	☐	☐
2.3.5.3	Ensure 'Domain controller: LDAP server channel binding token requirements' is set to 'Always' (DC Only) (Automated)	☐	☐
2.3.5.4	Ensure 'Domain controller: LDAP server signing requirements' is set to 'Require signing' (DC only) (Automated)	☐	☐
2.3.5.5	Ensure 'Domain controller: Refuse machine account password changes' is set to 'Disabled' (DC only) (Automated)	☐	☐
2.3.6	Domain member		
2.3.6.1	Ensure 'Domain member: Digitally encrypt or sign secure channel data (always)' is set to 'Enabled' (Automated)	☐	☐
2.3.6.2	Ensure 'Domain member: Digitally encrypt secure channel data (when possible)' is set to 'Enabled' (Automated)	☐	☐
2.3.6.3	Ensure 'Domain member: Digitally sign secure channel data (when possible)' is set to 'Enabled' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.6.4	Ensure 'Domain member: Disable machine account password changes' is set to 'Disabled' (Automated)	☐	☐
2.3.6.5	Ensure 'Domain member: Maximum machine account password age' is set to '30 or fewer days, but not 0' (Automated)	☐	☐
2.3.6.6	Ensure 'Domain member: Require strong (Windows 2000 or later) session key' is set to 'Enabled' (Automated)	☐	☐
2.3.7	Interactive logon		
2.3.7.1	Ensure 'Interactive logon: Do not display last user name' is set to 'Enabled' (Automated)	☐	☐
2.3.7.2	Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled' (Automated)	☐	☐
2.3.7.3	Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0' (Automated)	☐	☐
2.3.7.4	Configure 'Interactive logon: Message text for users attempting to log on' (Automated)	☐	☐
2.3.7.5	Configure 'Interactive logon: Message title for users attempting to log on' (Automated)	☐	☐
2.3.7.6	Ensure 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' is set to '4 or fewer logon(s)' (MS only) (Automated)	☐	☐
2.3.7.7	Ensure 'Interactive logon: Prompt user to change password before expiration' is set to 'between 5 and 14 days' (Automated)	☐	☐
2.3.7.8	Ensure 'Interactive logon: Require Domain Controller Authentication to unlock workstation' is set to 'Enabled' (MS only) (Automated)	☐	☐
2.3.7.9	Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.7.10	Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or 'Force Logoff' (STIG only) (Automated)	☐	☐
2.3.8	Microsoft network client		
2.3.8.1	Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled' (Automated)	☐	☐
2.3.8.2	Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled' (Automated)	☐	☐
2.3.8.3	Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled' (Automated)	☐	☐
2.3.9	Microsoft network server		
2.3.9.1	Ensure 'Microsoft network server: Amount of idle time required before suspending session' is set to '15 or fewer minute(s)' (Automated)	☐	☐
2.3.9.2	Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled' (Automated)	☐	☐
2.3.9.3	Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled' (Automated)	☐	☐
2.3.9.4	Ensure 'Microsoft network server: Disconnect clients when logon hours expire' is set to 'Enabled' (Automated)	☐	☐
2.3.9.5	Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher (MS only) (Automated)	☐	☐
2.3.10	Network access		
2.3.10.1	Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.10.2	Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled' (MS only) (Automated)	☐	☐
2.3.10.3	Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled' (STIG only) (Automated)	☐	☐
2.3.10.4	Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled' (MS only) (Automated)	☐	☐
2.3.10.5	Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled' (STIG only) (Automated)	☐	☐
2.3.10.6	Ensure 'Network access: Do not allow storage of passwords and credentials for network authentication' is set to 'Enabled' (Automated)	☐	☐
2.3.10.7	Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled' (Automated)	☐	☐
2.3.10.8	Configure 'Network access: Named Pipes that can be accessed anonymously' (DC only) (Automated)	☐	☐
2.3.10.9	Configure 'Network access: Named Pipes that can be accessed anonymously' (MS only) (Automated)	☐	☐
2.3.10.10	Configure 'Network access: Remotely accessible registry paths' is configured (Automated)	☐	☐
2.3.10.11	Configure 'Network access: Remotely accessible registry paths and sub-paths' is configured (Automated)	☐	☐
2.3.10.12	Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.10.13	Ensure 'Network access: Restrict clients allowed to make remote calls to SAM' is set to 'Administrators: Remote Access: Allow' (MS only) (Automated)	☐	☐
2.3.10.14	Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None' (Automated)	☐	☐
2.3.10.15	Ensure 'Network access: Sharing and security model for local accounts' is set to 'Classic - local users authenticate as themselves' (Automated)	☐	☐
2.3.11	Network security		
2.3.11.1	Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled' (Automated)	☐	☐
2.3.11.2	Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled' (Automated)	☐	☐
2.3.11.3	Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled' (Automated)	☐	☐
2.3.11.4	Ensure 'Network security: Configure encryption types allowed for Kerberos' is set to 'AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types' (Automated)	☐	☐
2.3.11.5	Ensure 'Network security: Do not store LAN Manager hash value on next password change' is set to 'Enabled' (Automated)	☐	☐
2.3.11.6	Ensure 'Network security: Force logoff when logon hours expire' is set to 'Enabled' (Manual)	☐	☐
2.3.11.7	Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.11.8	Ensure 'Network security: LDAP client signing requirements' is set to 'Negotiate signing' or higher (Automated)	☐	☐
2.3.11.9	Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit encryption' (Automated)	☐	☐
2.3.11.10	Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption' (Automated)	☐	☐
2.3.11.11	Ensure 'Network security: Restrict NTLM: Audit Incoming NTLM Traffic' is set to 'Enable auditing for all accounts' (Automated)	☐	☐
2.3.11.12	Ensure 'Network security: Restrict NTLM: Audit NTLM authentication in this domain' is set to 'Enable all' (DC only) (Automated)	☐	☐
2.3.11.13	Ensure 'Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers' is set to 'Audit all' or higher (Automated)	☐	☐
2.3.12	Recovery console		
2.3.13	Shutdown		
2.3.13.1	Ensure 'Shutdown: Allow system to be shut down without having to log on' is set to 'Disabled' (Automated)	☐	☐
2.3.14	System cryptography		
2.3.14.1	Ensure 'System cryptography: Force strong key protection for user keys stored on the computer' is set to 'User must enter a password each time they use a key' (STIG only) (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.14.2	Ensure 'System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing' is set to 'Enabled' (STIG only) (Automated)	☐	☐
2.3.15	System objects		
2.3.15.1	Ensure 'System objects: Require case insensitivity for non-Windows subsystems' is set to 'Enabled' (Automated)	☐	☐
2.3.15.2	Ensure 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)' is set to 'Enabled' (Automated)	☐	☐
2.3.16	System settings		
2.3.17	User Account Control		
2.3.17.1	Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled' (Automated)	☐	☐
2.3.17.2	Ensure 'User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop' is set to 'Disabled' (STIG only) (Automated)	☐	☐
2.3.17.3	Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop' or higher (Automated)	☐	☐
2.3.17.4	Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests' (Automated)	☐	☐
2.3.17.5	Ensure 'User Account Control: Detect application installations and prompt for elevation' is set to 'Enabled' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.17.6	Ensure 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' is set to 'Enabled' (Automated)	☐	☐
2.3.17.7	Ensure 'User Account Control: Run all administrators in Admin Approval Mode' is set to 'Enabled' (Automated)	☐	☐
2.3.17.8	Ensure 'User Account Control: Switch to the secure desktop when prompting for elevation' is set to 'Enabled' (Automated)	☐	☐
2.3.17.9	Ensure 'User Account Control: Virtualize file and registry write failures to per-user locations' is set to 'Enabled' (Automated)	☐	☐
3	Event Log		
4	Restricted Groups		
5	System Services		
5.1	Ensure 'Microsoft FTP Service (FTPSVC)' is set to 'Not Installed' (STIG only) (Automated)	☐	☐
5.2	Ensure 'Peer Name Resolution Protocol (PNRPsvc)' is set to 'Not Installed' (STIG only) (Automated)	☐	☐
5.3	Ensure 'Print Spooler (Spooler)' is set to 'Disabled' (DC only) (Automated)	☐	☐
5.4	Ensure 'Print Spooler (Spooler)' is set to 'Disabled' (MS only) (Automated)	☐	☐
5.5	Ensure 'Simple TCP/IP Services (simptcp)' is set to 'Not Installed' (Automated)	☐	☐
6	Registry		
7	File System		
8	Wired Network (IEEE 802.3) Policies		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
9	Windows Defender Firewall with Advanced Security (formerly Windows Firewall with Advanced Security)		
9.1	Domain Profile		
9.1.1	Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)' (Automated)	☐	☐
9.1.2	Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)' (Automated)	☐	☐
9.1.3	Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)' (STIG only) (Automated)	☐	☐
9.1.4	Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No' (Automated)	☐	☐
9.1.5	Ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\domainfw.log' (Automated)	☐	☐
9.1.6	Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater' (Automated)	☐	☐
9.1.7	Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes' (Automated)	☐	☐
9.1.8	Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes' (Automated)	☐	☐
9.2	Private Profile		
9.2.1	Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)' (Automated)	☐	☐
9.2.2	Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
9.2.3	Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)' (STIG only) (Automated)	☐	☐
9.2.4	Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No' (Automated)	☐	☐
9.2.5	Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\privatefw.log' (Automated)	☐	☐
9.2.6	Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater' (Automated)	☐	☐
9.2.7	Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes' (Automated)	☐	☐
9.2.8	Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes' (Automated)	☐	☐
9.3	Public Profile		
9.3.1	Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)' (Automated)	☐	☐
9.3.2	Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)' (Automated)	☐	☐
9.3.3	Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)' (STIG only) (Automated)	☐	☐
9.3.4	Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'No' (Automated)	☐	☐
9.3.5	Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No' (Automated)	☐	☐
9.3.6	Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
9.3.7	Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\publicfw.log' (Automated)	☐	☐
9.3.8	Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater' (Automated)	☐	☐
9.3.9	Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes' (Automated)	☐	☐
9.3.10	Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes' (Automated)	☐	☐
10	Network List Manager Policies		
11	Wireless Network (IEEE 802.11) Policies		
12	Public Key Policies		
13	Software Restriction Policies		
14	Network Access Protection NAP Client Configuration		
15	Application Control Policies		
16	IP Security Policies		
17	Advanced Audit Policy Configuration		
17.1	Account Logon		
17.1.1	Ensure 'Audit Credential Validation' is set to 'Success and Failure' (Automated)	☐	☐
17.1.2	Ensure 'Audit Kerberos Authentication Service' is set to 'Success and Failure' (DC Only) (Automated)	☐	☐
17.1.3	Ensure 'Audit Kerberos Service Ticket Operations' is set to 'Success and Failure' (DC Only) (Automated)	☐	☐
17.2	Account Management		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
17.2.1	Ensure 'Audit Application Group Management' is set to 'Success and Failure' (Automated)	☐	☐
17.2.2	Ensure 'Audit Computer Account Management' is set to include 'Success' (DC only) (Automated)	☐	☐
17.2.3	Ensure 'Audit Distribution Group Management' is set to include 'Success' (DC only) (Automated)	☐	☐
17.2.4	Ensure 'Audit Other Account Management Events' is set to include 'Success' (DC only) (Automated)	☐	☐
17.2.5	Ensure 'Audit Other Account Management Events' is set to include 'Success' (STIG Only) (Automated)	☐	☐
17.2.6	Ensure 'Audit Security Group Management' is set to include 'Success' (Automated)	☐	☐
17.2.7	Ensure 'Audit User Account Management' is set to 'Success and Failure' (Automated)	☐	☐
17.3	Detailed Tracking		
17.3.1	Ensure 'Audit PNP Activity' is set to include 'Success' (Automated)	☐	☐
17.3.2	Ensure 'Audit Process Creation' is set to include 'Success' (Automated)	☐	☐
17.4	DS Access		
17.4.1	Ensure 'Audit Directory Service Access' is set to include 'Failure' (DC only) (Automated)	☐	☐
17.4.2	Ensure 'Audit Directory Service Access' is set to include 'Success and Failure' (STIG DC only) (Automated)	☐	☐
17.4.3	Ensure 'Audit Directory Service Changes' is set to include 'Success' (DC only) (Automated)	☐	☐
17.5	Logon/Logoff		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
17.5.1	Ensure 'Audit Account Lockout' is set to include 'Failure' (Automated)	☐	☐
17.5.2	Ensure 'Audit Group Membership' is set to include 'Success' (Automated)	☐	☐
17.5.3	Ensure 'Audit Logoff' is set to include 'Success' (Automated)	☐	☐
17.5.4	Ensure 'Audit Logon' is set to 'Success and Failure' (Automated)	☐	☐
17.5.5	Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure' (Automated)	☐	☐
17.5.6	Ensure 'Audit Special Logon' is set to include 'Success' (Automated)	☐	☐
17.6	Object Access		
17.6.1	Ensure 'Audit Detailed File Share' is set to include 'Failure' (Automated)	☐	☐
17.6.2	Ensure 'Audit File Share' is set to 'Success and Failure' (Automated)	☐	☐
17.6.3	Ensure 'Audit Other Object Access Events' is set to 'Success and Failure' (Automated)	☐	☐
17.6.4	Ensure 'Audit Removable Storage' is set to 'Success and Failure' (Automated)	☐	☐
17.7	Policy Change		
17.7.1	Ensure 'Audit Audit Policy Change' is set to include 'Success' (Automated)	☐	☐
17.7.2	Ensure 'Audit Audit Policy Change' is set to include 'Success and Failure' (STIG only) (Automated)	☐	☐
17.7.3	Ensure 'Audit Authentication Policy Change' is set to include 'Success' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
17.7.4	Ensure 'Audit Authorization Policy Change' is set to include 'Success' (Automated)	☐	☐
17.7.5	Ensure 'Audit MPSSVC Rule-Level Policy Change' is set to 'Success and Failure' (Automated)	☐	☐
17.7.6	Ensure 'Audit Other Policy Change Events' is set to include 'Failure' (Automated)	☐	☐
17.8	Privilege Use		
17.8.1	Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure' (Automated)	☐	☐
17.9	System		
17.9.1	Ensure 'Audit IPsec Driver' is set to 'Success and Failure' (Automated)	☐	☐
17.9.2	Ensure 'Audit Other System Events' is set to 'Success and Failure' (Automated)	☐	☐
17.9.3	Ensure 'Audit Security State Change' is set to include 'Success' (Automated)	☐	☐
17.9.4	Ensure 'Audit Security System Extension' is set to include 'Success' (Automated)	☐	☐
17.9.5	Ensure 'Audit System Integrity' is set to 'Success and Failure' (Automated)	☐	☐
18	Administrative Templates (Computer)		
18.1	Control Panel		
18.1.1	Personalization		
18.1.1.1	Ensure 'Prevent enabling lock screen camera' is set to 'Enabled' (Automated)	☐	☐
18.1.1.2	Ensure 'Prevent enabling lock screen slide show' is set to 'Enabled' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.1.2	Regional and Language Options		
18.1.2.1	Handwriting personalization		
18.1.2.2	Ensure 'Allow users to enable online speech recognition services' is set to 'Disabled' (Automated)	☐	☐
18.1.3	Ensure 'Allow Online Tips' is set to 'Disabled' (Automated)	☐	☐
18.2	Desktop		
18.3	LAPS (legacy)		
18.3.1	Ensure LAPS AdmPwd GPO Extension / CSE is installed (MS only) (Automated)	☐	☐
18.3.2	Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled' (MS only) (Automated)	☐	☐
18.3.3	Ensure 'Enable Local Admin Password Management' is set to 'Enabled' (MS only) (Automated)	☐	☐
18.3.4	Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + special characters' (MS only) (Automated)	☐	☐
18.3.5	Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more' (MS only) (Automated)	☐	☐
18.3.6	Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer' (MS only) (Automated)	☐	☐
18.3.7	Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 60 or fewer' (STIG MS only) (Automated)	☐	☐
18.4	MS Security Guide		
18.4.1	Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled' (MS only) (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.4.2	Ensure 'Configure RPC packet level privacy setting for incoming connections' is set to 'Enabled' (Automated)	☐	☐
18.4.3	Ensure 'Configure SMB v1 client driver' is set to 'Enabled: Disable driver (recommended)' (Automated)	☐	☐
18.4.4	Ensure 'Configure SMB v1 server' is set to 'Disabled' (Automated)	☐	☐
18.4.5	Ensure 'Enable Certificate Padding' is set to 'Enabled' (Automated)	☐	☐
18.4.6	Ensure 'Enable Structured Exception Handling Overwrite Protection (SEHOP)' is set to 'Enabled' (Automated)	☐	☐
18.4.7	Ensure 'LSA Protection' is set to 'Enabled' (Automated)	☐	☐
18.4.8	Ensure 'NetBT NodeType configuration' is set to 'Enabled: P-node (recommended)' (Automated)	☐	☐
18.4.9	Ensure 'WDigest Authentication' is set to 'Disabled' (Automated)	☐	☐
18.5	MSS (Legacy)		
18.5.1	Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon' is set to 'Disabled' (Automated)	☐	☐
18.5.2	Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level' is set to 'Enabled: Highest protection, source routing is completely disabled' (Automated)	☐	☐
18.5.3	Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level' is set to 'Enabled: Highest protection, source routing is completely disabled' (Automated)	☐	☐
18.5.4	Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.5.5	Ensure 'MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds' is set to 'Enabled: 300,000 or 5 minutes' (Automated)	☐	☐
18.5.6	Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled' (Automated)	☐	☐
18.5.7	Ensure 'MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses' is set to 'Disabled' (Automated)	☐	☐
18.5.8	Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode' is set to 'Enabled' (Automated)	☐	☐
18.5.9	Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires' is set to 'Enabled: 5 or fewer seconds' (Automated)	☐	☐
18.5.10	Ensure 'MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3' (Automated)	☐	☐
18.5.11	Ensure 'MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3' (Automated)	☐	☐
18.5.12	Ensure 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' is set to 'Enabled: 90% or less' (Automated)	☐	☐
18.6	Network		
18.6.1	Background Intelligent Transfer Service (BITS)		
18.6.2	BranchCache		
18.6.3	DirectAccess Client Experience Settings		
18.6.4	DNS Client		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.6.4.1	Ensure 'Configure NetBIOS settings' is set to 'Enabled: Disable NetBIOS name resolution on public networks' (Automated)	☐	☐
18.6.4.2	Ensure 'Turn off multicast name resolution' is set to 'Enabled' (Automated)	☐	☐
18.6.5	Fonts		
18.6.5.1	Ensure 'Enable Font Providers' is set to 'Disabled' (Automated)	☐	☐
18.6.6	Hotspot Authentication		
18.6.7	Lanman Server		
18.6.8	Lanman Workstation		
18.6.8.1	Ensure 'Enable insecure guest logons' is set to 'Disabled' (Automated)	☐	☐
18.6.9	Link-Layer Topology Discovery		
18.6.9.1	Ensure 'Turn on Mapper I/O (LLTDIO) driver' is set to 'Disabled' (Automated)	☐	☐
18.6.9.2	Ensure 'Turn on Responder (RSPNDR) driver' is set to 'Disabled' (Automated)	☐	☐
18.6.10	Microsoft Peer-to-Peer Networking Services		
18.6.10.1	Peer Name Resolution Protocol		
18.6.10.2	Ensure 'Turn off Microsoft Peer-to-Peer Networking Services' is set to 'Enabled' (Automated)	☐	☐
18.6.11	Network Connections		
18.6.11.1	Windows Defender Firewall (formerly Windows Firewall)		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.6.11.2	Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled' (Automated)	☐	☐
18.6.11.3	Ensure 'Prohibit use of Internet Connection Sharing on your DNS domain network' is set to 'Enabled' (Automated)	☐	☐
18.6.11.4	Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled' (Automated)	☐	☐
18.6.12	Network Connectivity Status Indicator		
18.6.13	Network Isolation		
18.6.14	Network Provider		
18.6.14.1	Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication", "Require Integrity", and "Require Privacy" set for all NETLOGON and SYSVOL shares' (Automated)	☐	☐
18.6.14.2	Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication", "Require Integrity" set for all NETLOGON and SYSVOL shares' (STIG only) (Automated)	☐	☐
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		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.6.19.2.1	Disable IPv6 (Ensure TCPIP6 Parameter 'DisabledComponents' is set to '0xff (255)') (Automated)	☐	☐
18.6.20	Windows Connect Now		
18.6.20.1	Ensure 'Configuration of wireless settings using Windows Connect Now' is set to 'Disabled' (Automated)	☐	☐
18.6.20.2	Ensure 'Prohibit access of the Windows Connect Now wizards' is set to 'Enabled' (Automated)	☐	☐
18.6.21	Windows Connection Manager		
18.6.21.1	Ensure 'Minimize the number of simultaneous connections to the Internet or a Windows Domain' is set to 'Enabled: 1 = Minimize simultaneous connections' (Automated)	☐	☐
18.6.21.2	Ensure 'Prohibit connection to non-domain networks when connected to domain authenticated network' is set to 'Enabled' (MS only) (Automated)	☐	☐
18.7	Printers		
18.7.1	Ensure 'Allow Print Spooler to accept client connections' is set to 'Disabled' (Automated)	☐	☐
18.7.2	Ensure 'Configure Redirection Guard' is set to 'Enabled: Redirection Guard Enabled' (Automated)	☐	☐
18.7.3	Ensure 'Configure RPC connection settings: Protocol to use for outgoing RPC connections' is set to 'Enabled: RPC over TCP' (Automated)	☐	☐
18.7.4	Ensure 'Configure RPC connection settings: Use authentication for outgoing RPC connections' is set to 'Enabled: Default' (Automated)	☐	☐
18.7.5	Ensure 'Configure RPC listener settings: Protocols to allow for incoming RPC connections' is set to 'Enabled: RPC over TCP' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.7.6	Ensure 'Configure RPC listener settings: Authentication protocol to use for incoming RPC connections:' is set to 'Enabled: Negotiate' or higher (Automated)	☐	☐
18.7.7	Ensure 'Configure RPC over TCP port' is set to 'Enabled: 0' (Automated)	☐	☐
18.7.8	Ensure 'Limits print driver installation to Administrators' is set to 'Enabled' (Automated)	☐	☐
18.7.9	Ensure 'Manage processing of Queue-specific files' is set to 'Enabled: Limit Queue-specific files to Color profiles' (Automated)	☐	☐
18.7.10	Ensure 'Point and Print Restrictions: When installing drivers for a new connection' is set to 'Enabled: Show warning and elevation prompt' (Automated)	☐	☐
18.7.11	Ensure 'Point and Print Restrictions: When updating drivers for an existing connection' is set to 'Enabled: Show warning and elevation prompt' (Automated)	☐	☐
18.8	Start Menu and Taskbar		
18.8.1	Notifications		
18.8.1.1	Ensure 'Turn off notifications network usage' is set to 'Enabled' (Automated)	☐	☐
18.9	System		
18.9.1	Access-Denied Assistance		
18.9.2	App-V		
18.9.3	Audit Process Creation		
18.9.3.1	Ensure 'Include command line in process creation events' is set to 'Enabled' (Automated)	☐	☐
18.9.4	Credentials Delegation		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.9.4.1	Ensure 'Encryption Oracle Remediation' is set to 'Enabled: Force Updated Clients' (Automated)	☐	☐
18.9.4.2	Ensure 'Remote host allows delegation of non-exportable credentials' is set to 'Enabled' (Automated)	☐	☐
18.9.5	Device Guard		
18.9.5.1	Ensure 'Turn On Virtualization Based Security' is set to 'Enabled' (Automated)	☐	☐
18.9.5.2	Ensure 'Turn On Virtualization Based Security: Select Platform Security Level' is set to 'Secure Boot' or higher (Automated)	☐	☐
18.9.5.3	Ensure 'Turn On Virtualization Based Security: Virtualization Based Protection of Code Integrity' is set to 'Enabled with UEFI lock' (Automated)	☐	☐
18.9.5.4	Ensure 'Turn On Virtualization Based Security: Require UEFI Memory Attributes Table' is set to 'True (checked)' (Automated)	☐	☐
18.9.5.5	Ensure 'Turn On Virtualization Based Security: Credential Guard Configuration' is set to 'Enabled with UEFI lock' (MS Only) (Automated)	☐	☐
18.9.5.6	Ensure 'Turn On Virtualization Based Security: Credential Guard Configuration' is set to 'Disabled' (DC Only) (Automated)	☐	☐
18.9.5.7	Ensure 'Turn On Virtualization Based Security: Secure Launch Configuration' is set to 'Enabled' (Automated)	☐	☐
18.9.6	Device Health Attestation Service		
18.9.7	Device Installation		
18.9.7.1	Device Installation Restrictions		
18.9.7.2	Ensure 'Prevent device metadata retrieval from the Internet' is set to 'Enabled' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.9.8	Disk NV Cache		
18.9.9	Disk Quotas		
18.9.10	Display		
18.9.11	Distributed COM		
18.9.12	Driver Installation		
18.9.13	Early Launch Antimalware		
18.9.13.1	Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good, unknown and bad but critical' (Automated)	☐	☐
18.9.13.2	Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: any, but ALL' (STIG only) (Automated)	☐	☐
18.9.14	Enhanced Storage Access		
18.9.15	File Classification Infrastructure		
18.9.16	File Share Shadow Copy Provider		
18.9.17	Filesystem (formerly NTFS Filesystem)		
18.9.18	Folder Redirection		
18.9.19	Group Policy		
18.9.19.1	Logging and tracing		
18.9.19.2	Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE' (Automated)	☐	☐
18.9.19.3	Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.9.19.4	Ensure 'Configure security policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE' (Automated)	☐	☐
18.9.19.5	Ensure 'Configure security policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE' (Automated)	☐	☐
18.9.19.6	Ensure 'Continue experiences on this device' is set to 'Disabled' (Automated)	☐	☐
18.9.19.7	Ensure 'Turn off background refresh of Group Policy' is set to 'Disabled' (Automated)	☐	☐
18.9.20	Internet Communication Management		
18.9.20.1	Internet Communication settings		
18.9.20.1.1	Ensure 'Turn off downloading of print drivers over HTTP' is set to 'Enabled' (Automated)	☐	☐
18.9.20.1.2	Ensure 'Turn off handwriting personalization data sharing' is set to 'Enabled' (Automated)	☐	☐
18.9.20.1.3	Ensure 'Turn off handwriting recognition error reporting' is set to 'Enabled' (Automated)	☐	☐
18.9.20.1.4	Ensure 'Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com' is set to 'Enabled' (Automated)	☐	☐
18.9.20.1.5	Ensure 'Turn off Internet download for Web publishing and online ordering wizards' is set to 'Enabled' (Automated)	☐	☐
18.9.20.1.6	Ensure 'Turn off printing over HTTP' is set to 'Enabled' (Automated)	☐	☐
18.9.20.1.7	Ensure 'Turn off Registration if URL connection is referring to Microsoft.com' is set to 'Enabled' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.9.20.1.8	Ensure 'Turn off Search Companion content file updates' is set to 'Enabled' (Automated)	☐	☐
18.9.20.1.9	Ensure 'Turn off the "Order Prints" picture task' is set to 'Enabled' (Automated)	☐	☐
18.9.20.1.10	Ensure 'Turn off the "Publish to Web" task for files and folders' is set to 'Enabled' (Automated)	☐	☐
18.9.20.1.11	Ensure 'Turn off the Windows Messenger Customer Experience Improvement Program' is set to 'Enabled' (Automated)	☐	☐
18.9.20.1.12	Ensure 'Turn off Windows Customer Experience Improvement Program' is set to 'Enabled' (Automated)	☐	☐
18.9.20.1.13	Ensure 'Turn off Windows Error Reporting' is set to 'Enabled' (Automated)	☐	☐
18.9.21	iSCSI		
18.9.22	KDC		
18.9.23	Kerberos		
18.9.23.1	Ensure 'Support device authentication using certificate' is set to 'Enabled: Automatic' (Automated)	☐	☐
18.9.24	Kernel DMA Protection		
18.9.25	LAPS		
18.9.26	Local Security Authority		
18.9.27	Locale Services		
18.9.27.1	Ensure 'Disallow copying of user input methods to the system account for sign-in' is set to 'Enabled' (Automated)	☐	☐
18.9.28	Logon		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.9.28.1	Ensure 'Block user from showing account details on sign-in' is set to 'Enabled' (Automated)	☐	☐
18.9.28.2	Ensure 'Do not display network selection UI' is set to 'Enabled' (Automated)	☐	☐
18.9.28.3	Ensure 'Do not enumerate connected users on domain-joined computers' is set to 'Enabled' (Automated)	☐	☐
18.9.28.4	Ensure 'Enumerate local users on domain-joined computers' is set to 'Disabled' (MS only) (Automated)	☐	☐
18.9.28.5	Ensure 'Turn off app notifications on the lock screen' is set to 'Enabled' (Automated)	☐	☐
18.9.28.6	Ensure 'Turn off picture password sign-in' is set to 'Enabled' (Automated)	☐	☐
18.9.28.7	Ensure 'Turn on convenience PIN sign-in' is set to 'Disabled' (Automated)	☐	☐
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		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.9.33.6.1	Ensure 'Allow network connectivity during connected-standby (on battery)' is set to 'Disabled' (Automated)	☐	☐
18.9.33.6.2	Ensure 'Allow network connectivity during connected-standby (plugged in)' is set to 'Disabled' (Automated)	☐	☐
18.9.33.6.3	Ensure 'Require a password when a computer wakes (on battery)' is set to 'Enabled' (Automated)	☐	☐
18.9.33.6.4	Ensure 'Require a password when a computer wakes (plugged in)' is set to 'Enabled' (Automated)	☐	☐
18.9.34	Recovery		
18.9.35	Remote Assistance		
18.9.35.1	Ensure 'Configure Offer Remote Assistance' is set to 'Disabled' (Automated)	☐	☐
18.9.35.2	Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled' (Automated)	☐	☐
18.9.36	Remote Procedure Call		
18.9.36.1	Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled' (MS only) (Automated)	☐	☐
18.9.36.2	Ensure 'Restrict Unauthenticated RPC clients' is set to 'Enabled: Authenticated' (MS only) (Automated)	☐	☐
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		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
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		
18.9.47.3	Disk Diagnostic		
18.9.47.4	Fault Tolerant Heap		
18.9.47.5	Microsoft Support Diagnostic Tool		
18.9.47.5.1	Ensure 'Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider' is set to 'Disabled' (Automated)	☐	☐
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		
18.9.47.11.1	Ensure 'Enable/Disable PerfTrack' is set to 'Disabled' (Automated)	☐	☐
18.9.48	Trusted Platform Module Services		
18.9.49	User Profiles		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.9.49.1	Ensure 'Turn off the advertising ID' is set to 'Enabled' (Automated)	☐	☐
18.9.50	Windows File Protection		
18.9.51	Windows Time Service		
18.9.51.1	Time Providers		
18.9.51.1.1	Ensure 'Enable Windows NTP Client' is set to 'Enabled' (Automated)	☐	☐
18.9.51.1.2	Ensure 'Enable Windows NTP Client' is set to 'Enabled: DoD time server' (STIG only) (Automated)	☐	☐
18.9.51.1.3	Ensure 'Enable Windows NTP Server' is set to 'Disabled' (MS only) (Automated)	☐	☐
18.10	Windows Components		
18.10.1	ActiveX Installer Service		
18.10.2	Add features to Windows 10 (formerly Windows Anytime Upgrade)		
18.10.3	App Package Deployment		
18.10.3.1	Ensure 'Allow a Windows app to share application data between users' is set to 'Disabled' (Automated)	☐	☐
18.10.4	App Privacy		
18.10.5	App runtime		
18.10.5.1	Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled' (Automated)	☐	☐
18.10.6	Application Compatibility		
18.10.6.1	Ensure 'Turn off Inventory Collector' is set to 'Enabled' (STIG only) (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.10.7	AutoPlay Policies		
18.10.7.1	Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled' (Automated)	☐	☐
18.10.7.2	Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands' (Automated)	☐	☐
18.10.7.3	Ensure 'Turn off Autoplay' is set to 'Enabled: All drives' (Automated)	☐	☐
18.10.8	Biometrics		
18.10.8.1	Facial Features		
18.10.8.1.1	Ensure 'Configure enhanced anti-spoofing' is set to 'Enabled' (Automated)	☐	☐
18.10.9	BitLocker Drive Encryption		
18.10.10	Camera		
18.10.10.1	Ensure 'Allow Use of Camera' is set to 'Disabled' (Automated)	☐	☐
18.10.11	Chat		
18.10.12	Cloud Content		
18.10.12.1	Ensure 'Turn off cloud consumer account state content' is set to 'Enabled' (Automated)	☐	☐
18.10.12.2	Ensure 'Turn off Microsoft consumer experiences' is set to 'Enabled' (Automated)	☐	☐
18.10.13	Connect		
18.10.13.1	Ensure 'Require pin for pairing' is set to 'Enabled: First Time' OR 'Enabled: Always' (Automated)	☐	☐
18.10.14	Credential User Interface		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.10.14.1	Ensure 'Do not display the password reveal button' is set to 'Enabled' (Automated)	☐	☐
18.10.14.2	Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled' (Automated)	☐	☐
18.10.15	Data Collection and Preview Builds		
18.10.15.1	Ensure 'Allow Diagnostic Data' is set to 'Enabled: Diagnostic data off (not recommended)' or 'Enabled: Send required diagnostic data' (Automated)	☐	☐
18.10.15.2	Ensure 'Configure Authenticated Proxy usage for the Connected User Experience and Telemetry service' is set to 'Enabled: Disable Authenticated Proxy usage' (Automated)	☐	☐
18.10.15.3	Ensure 'Disable OneSettings Downloads' is set to 'Enabled' (Automated)	☐	☐
18.10.15.4	Ensure 'Do not show feedback notifications' is set to 'Enabled' (Automated)	☐	☐
18.10.15.5	Ensure 'Enable OneSettings Auditing' is set to 'Enabled' (Automated)	☐	☐
18.10.15.6	Ensure 'Limit Diagnostic Log Collection' is set to 'Enabled' (Automated)	☐	☐
18.10.15.7	Ensure 'Limit Dump Collection' is set to 'Enabled' (Automated)	☐	☐
18.10.15.8	Ensure 'Toggle user control over Insider builds' is set to 'Disabled' (Automated)	☐	☐
18.10.16	Delivery Optimization		
18.10.17	Desktop App Installer		
18.10.18	Desktop Gadgets		
18.10.19	Desktop Window Manager		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.10.20	Device and Driver Compatibility		
18.10.21	Device Registration (formerly Workplace Join)		
18.10.22	Digital Locker		
18.10.23	Edge UI		
18.10.24	Event Forwarding		
18.10.25	Event Log Service		
18.10.25.1	Application		
18.10.25.1.1	Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated)	☐	☐
18.10.25.1.2	Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Automated)	☐	☐
18.10.25.2	Security		
18.10.25.2.1	Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated)	☐	☐
18.10.25.2.2	Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater' (Automated)	☐	☐
18.10.25.3	Setup		
18.10.25.3.1	Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated)	☐	☐
18.10.25.3.2	Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Automated)	☐	☐
18.10.25.4	System		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.10.25.4.1	Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated)	☐	☐
18.10.25.4.2	Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Automated)	☐	☐
18.10.26	Event Logging		
18.10.27	Event Viewer		
18.10.28	File Explorer (formerly Windows Explorer)		
18.10.28.1	Previous Versions		
18.10.28.2	Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled' (Automated)	☐	☐
18.10.28.3	Ensure 'Turn off heap termination on corruption' is set to 'Disabled' (Automated)	☐	☐
18.10.28.4	Ensure 'Turn off shell protocol protected mode' is set to 'Disabled' (Automated)	☐	☐
18.10.29	File History		
18.10.30	Find My Device		
18.10.31	Handwriting		
18.10.32	HomeGroup		
18.10.33	Human Presence		
18.10.34	Internet Explorer		
18.10.35	Internet Information Services		
18.10.36	Location and Sensors		
18.10.36.1	Ensure 'Turn off location' is set to 'Enabled' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.10.37	Maintenance Scheduler		
18.10.38	Maps		
18.10.39	MDM		
18.10.40	Messaging		
18.10.40.1	Ensure 'Allow Message Service Cloud Sync' is set to 'Disabled' (Automated)	☐	☐
18.10.41	Microsoft account		
18.10.41.1	Ensure 'Block all consumer Microsoft account user authentication' is set to 'Enabled' (Automated)	☐	☐
18.10.42	Microsoft Defender Antivirus (formerly Windows Defender and Windows Defender Antivirus)		
18.10.42.1	Client Interface		
18.10.42.2	Device Control		
18.10.42.3	Exclusions		
18.10.42.4	Features		
18.10.42.5	MAPS		
18.10.42.5.1	Ensure 'Configure local setting override for reporting to Microsoft MAPS' is set to 'Disabled' (Automated)	☐	☐
18.10.42.5.2	Ensure 'Join Microsoft MAPS' is set to 'Disabled' (Automated)	☐	☐
18.10.42.6	Microsoft Defender Exploit Guard (formerly Windows Defender Exploit Guard)		
18.10.42.6.1	Attack Surface Reduction		
18.10.42.6.1.1	Ensure 'Configure Attack Surface Reduction rules' is set to 'Enabled' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.10.42.6.1.2	Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is configured (Automated)	☐	☐
18.10.42.6.2	Controlled Folder Access		
18.10.42.6.3	Network Protection		
18.10.42.6.3.1	Ensure 'Prevent users and apps from accessing dangerous websites' is set to 'Enabled: Block' (Automated)	☐	☐
18.10.42.7	MpEngine		
18.10.42.7.1	Ensure 'Enable file hash computation feature' is set to 'Enabled' (Automated)	☐	☐
18.10.42.8	Network Inspection System		
18.10.42.9	Quarantine		
18.10.42.10	Real-time Protection		
18.10.42.10.1	Ensure 'Scan all downloaded files and attachments' is set to 'Enabled' (Automated)	☐	☐
18.10.42.10.2	Ensure 'Turn off real-time protection' is set to 'Disabled' (Automated)	☐	☐
18.10.42.10.3	Ensure 'Turn on behavior monitoring' is set to 'Enabled' (Automated)	☐	☐
18.10.42.10.4	Ensure 'Turn on script scanning' is set to 'Enabled' (Automated)	☐	☐
18.10.42.11	Remediation		
18.10.42.12	Reporting		
18.10.42.12.1	Ensure 'Configure Watson events' is set to 'Disabled' (Automated)	☐	☐
18.10.42.13	Scan		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.10.42.13.1	Ensure 'Scan packed executables' is set to 'Enabled' (Automated)	☐	☐
18.10.42.13.2	Ensure 'Scan removable drives' is set to 'Enabled' (Automated)	☐	☐
18.10.42.13.3	Ensure 'Turn on e-mail scanning' is set to 'Enabled' (Automated)	☐	☐
18.10.42.14	Security Intelligence Updates (formerly Signature Updates)		
18.10.42.15	Threats		
18.10.42.16	Ensure 'Configure detection for potentially unwanted applications' is set to 'Enabled: Block' (Automated)	☐	☐
18.10.42.17	Ensure 'Turn off Microsoft Defender AntiVirus' is set to 'Disabled' (Automated)	☐	☐
18.10.43	Microsoft Defender Application Guard (formerly Windows Defender Application Guard)		
18.10.44	Microsoft Defender Exploit Guard (formerly Windows Defender Exploit Guard)		
18.10.45	Microsoft Edge		
18.10.46	Microsoft Secondary Authentication Factor		
18.10.47	Microsoft User Experience Virtualization		
18.10.48	NetMeeting		
18.10.49	News and interests		
18.10.50	OneDrive (formerly SkyDrive)		
18.10.50.1	Ensure 'Prevent the usage of OneDrive for file storage' is set to 'Enabled' (Automated)	☐	☐
18.10.51	Online Assistance		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.10.52	OOBE		
18.10.53	Portable Operating System		
18.10.54	Presentation Settings		
18.10.55	Push To Install		
18.10.55.1	Ensure 'Turn off Push To Install service' is set to 'Enabled' (Automated)	☐	☐
18.10.56	Remote Desktop Services (formerly Terminal Services)		
18.10.56.1	RD Licensing (formerly TS Licensing)		
18.10.56.2	Remote Desktop Connection Client		
18.10.56.2.1	RemoteFX USB Device Redirection		
18.10.56.2.2	Ensure 'Do not allow passwords to be saved' is set to 'Enabled' (Automated)	☐	☐
18.10.56.3	Remote Desktop Session Host (formerly Terminal Server)		
18.10.56.3.1	Application Compatibility		
18.10.56.3.2	Connections		
18.10.56.3.2.1	Ensure 'Restrict Remote Desktop Services users to a single Remote Desktop Services session' is set to 'Enabled' (Automated)	☐	☐
18.10.56.3.3	Device and Resource Redirection		
18.10.56.3.3.1	Ensure 'Do not allow COM port redirection' is set to 'Enabled' (Automated)	☐	☐
18.10.56.3.3.2	Ensure 'Do not allow drive redirection' is set to 'Enabled' (Automated)	☐	☐
18.10.56.3.3.3	Ensure 'Do not allow LPT port redirection' is set to 'Enabled' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.10.56.3.3.4	Ensure 'Do not allow supported Plug and Play device redirection' is set to 'Enabled' (Automated)	☐	☐
18.10.56.3.4	Licensing		
18.10.56.3.5	Printer Redirection		
18.10.56.3.6	Profiles		
18.10.56.3.7	RD Connection Broker (formerly TS Connection Broker)		
18.10.56.3.8	Remote Session Environment		
18.10.56.3.9	Security		
18.10.56.3.9.1	Ensure 'Always prompt for password upon connection' is set to 'Enabled' (Automated)	☐	☐
18.10.56.3.9.2	Ensure 'Require secure RPC communication' is set to 'Enabled' (Automated)	☐	☐
18.10.56.3.9.3	Ensure 'Require use of specific security layer for remote (RDP) connections' is set to 'Enabled: SSL' (Automated)	☐	☐
18.10.56.3.9.4	Ensure 'Require user authentication for remote connections by using Network Level Authentication' is set to 'Enabled' (Automated)	☐	☐
18.10.56.3.9.5	Ensure 'Set client connection encryption level' is set to 'Enabled: High Level' (Automated)	☐	☐
18.10.56.3.10	Session Time Limits		
18.10.56.3.10.1	Ensure 'Set time limit for active but idle Remote Desktop Services sessions' is set to 'Enabled: 15 minutes or less, but not Never (0)' (Automated)	☐	☐
18.10.56.3.10.2	Ensure 'Set time limit for disconnected sessions' is set to 'Enabled: 1 minute' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.10.56.3.1	Temporary folders		
18.10.56.3.1 1.1	Ensure 'Do not delete temp folders upon exit' is set to 'Disabled' (Automated)	☐	☐
18.10.56.3.1 1.2	Ensure 'Do not use temporary folders per session' is set to 'Disabled' (Automated)	☐	☐
18.10.57	RSS Feeds		
18.10.57.1	Ensure 'Prevent downloading of enclosures' is set to 'Enabled' (Automated)	☐	☐
18.10.57.2	Ensure 'Turn on Basic feed authentication over HTTP' is set to 'Not configured' or 'Disabled' (STIG only) (Automated)	☐	☐
18.10.58	Search		
18.10.58.1	OCR		
18.10.58.2	Ensure 'Allow Cloud Search' is set to 'Enabled: Disable Cloud Search' (Automated)	☐	☐
18.10.58.3	Ensure 'Allow indexing of encrypted files' is set to 'Disabled' (Automated)	☐	☐
18.10.58.4	Ensure 'Allow search highlights' is set to 'Disabled' (Automated)	☐	☐
18.10.59	Security Center		
18.10.60	Shutdown Options		
18.10.61	Smart Card		
18.10.62	Software Protection Platform		
18.10.62.1	Ensure 'Turn off KMS Client Online AVS Validation' is set to 'Enabled' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.10.63	Sound Recorder		
18.10.64	Speech		
18.10.65	Store		
18.10.66	Sync your settings		
18.10.67	Tablet PC		
18.10.68	Task Scheduler		
18.10.69	Tenant Restrictions		
18.10.70	Text Input		
18.10.71	Widgets		
18.10.72	Windows Calendar		
18.10.73	Windows Color System		
18.10.74	Windows Customer Experience Improvement Program		
18.10.75	Windows Defender SmartScreen		
18.10.75.1	Enhanced Phishing Protection		
18.10.75.2	Explorer		
18.10.75.2.1	Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled: Warn and prevent bypass' (Automated)	☐	☐
18.10.75.2.2	Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled' (STIG only) (Automated)	☐	☐
18.10.76	Windows Error Reporting		
18.10.77	Windows Game Recording and Broadcasting		
18.10.78	Windows Hello for Business (formerly Microsoft Passport for Work)		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.10.79	Windows Ink Workspace		
18.10.79.1	Ensure 'Allow suggested apps in Windows Ink Workspace' is set to 'Disabled' (Automated)	☐	☐
18.10.79.2	Ensure 'Allow Windows Ink Workspace' is set to 'Enabled: On, but disallow access above lock' OR 'Enabled: Disabled' (Automated)	☐	☐
18.10.80	Windows Installer		
18.10.80.1	Ensure 'Allow user control over installs' is set to 'Disabled' (Automated)	☐	☐
18.10.80.2	Ensure 'Always install with elevated privileges' is set to 'Disabled' (Automated)	☐	☐
18.10.80.3	Ensure 'Prevent Internet Explorer security prompt for Windows Installer scripts' is set to 'Disabled' (Automated)	☐	☐
18.10.81	Windows Logon Options		
18.10.81.1	Ensure 'Sign-in and lock last interactive user automatically after a restart' is set to 'Disabled' (Automated)	☐	☐
18.10.82	Windows Media Digital Rights Management		
18.10.83	Windows Media Player		
18.10.84	Windows Messenger		
18.10.85	Windows Mobility Center		
18.10.86	Windows PowerShell		
18.10.86.1	Ensure 'Turn on PowerShell Script Block Logging' is set to 'Enabled' (Automated)	☐	☐
18.10.86.2	Ensure 'Turn on PowerShell Transcription' is set to 'Enabled' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.10.87	Windows Reliability Analysis		
18.10.88	Windows Remote Management (WinRM)		
18.10.88.1	WinRM Client		
18.10.88.1.1	Ensure 'Allow Basic authentication' is set to 'Disabled' (Automated)	☐	☐
18.10.88.1.2	Ensure 'Allow unencrypted traffic' is set to 'Disabled' (Automated)	☐	☐
18.10.88.1.3	Ensure 'Disallow Digest authentication' is set to 'Enabled' (Automated)	☐	☐
18.10.88.2	WinRM Service		
18.10.88.2.1	Ensure 'Allow Basic authentication' is set to 'Disabled' (Automated)	☐	☐
18.10.88.2.2	Ensure 'Allow remote server management through WinRM' is set to 'Disabled' (Automated)	☐	☐
18.10.88.2.3	Ensure 'Allow unencrypted traffic' is set to 'Disabled' (Automated)	☐	☐
18.10.88.2.4	Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled' (Automated)	☐	☐
18.10.89	Windows Remote Shell		
18.10.89.1	Ensure 'Allow Remote Shell Access' is set to 'Disabled' (Automated)	☐	☐
18.10.90	Windows Sandbox		
18.10.91	Windows Security (formerly Windows Defender Security Center)		
18.10.91.1	Account protection		
18.10.91.2	App and browser protection		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.10.91.2.1	Ensure 'Prevent users from modifying settings' is set to 'Enabled' (Automated)	☐	☐
18.10.92	Windows Update		
18.10.92.1	Legacy Policies		
18.10.92.1.1	Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled' (Automated)	☐	☐
18.10.92.2	Manage end user experience		
18.10.92.2.1	Ensure 'Configure Automatic Updates' is set to 'Enabled' (Automated)	☐	☐
18.10.92.2.2	Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day' (Automated)	☐	☐
18.10.92.3	Manage updates offered from Windows Server Update Service		
18.10.92.4	Manage updates offered from Windows Update (formerly Defer Windows Updates and Windows Update for Business)		
18.10.92.4.1	Ensure 'Manage preview builds' is set to 'Disabled' (Automated)	☐	☐
18.10.92.4.2	Ensure 'Select when Preview Builds and Feature Updates are received' is set to 'Enabled: 180 or more days' (Automated)	☐	☐
18.10.92.4.3	Ensure 'Select when Quality Updates are received' is set to 'Enabled: 0 days' (Automated)	☐	☐
19	Administrative Templates (User)		
19.1	Control Panel		
19.2	Desktop		
19.3	Network		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
19.4	Shared Folders		
19.5	Start Menu and Taskbar		
19.5.1	Notifications		
19.5.1.1	Ensure 'Turn off toast notifications on the lock screen' is set to 'Enabled' (Automated)	☐	☐
19.6	System		
19.6.1	Ctrl+Alt+Del Options		
19.6.2	Display		
19.6.3	Driver Installation		
19.6.4	Folder Redirection		
19.6.5	Group Policy		
19.6.6	Internet Communication Management		
19.6.6.1	Internet Communication settings		
19.6.6.1.1	Ensure 'Turn off Help Experience Improvement Program' is set to 'Enabled' (Automated)	☐	☐
19.7	Windows Components		
19.7.1	Account Notifications		
19.7.2	Add features to Windows 8 / 8.1 / 10 (formerly Windows Anytime Upgrade)		
19.7.3	App runtime		
19.7.4	Application Compatibility		
19.7.5	Attachment Manager		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
19.7.5.1	Ensure 'Do not preserve zone information in file attachments' is set to 'Disabled' (Automated)	☐	☐
19.7.5.2	Ensure 'Notify antivirus programs when opening attachments' is set to 'Enabled' (Automated)	☐	☐
19.7.6	AutoPlay Policies		
19.7.7	Calculator		
19.7.8	Cloud Content		
19.7.8.1	Ensure 'Configure Windows spotlight on lock screen' is set to 'Disabled' (Automated)	☐	☐
19.7.8.2	Ensure 'Do not suggest third-party content in Windows spotlight' is set to 'Enabled' (Automated)	☐	☐
19.7.8.3	Ensure 'Do not use diagnostic data for tailored experiences' is set to 'Enabled' (Automated)	☐	☐
19.7.8.4	Ensure 'Turn off all Windows spotlight features' is set to 'Enabled' (Automated)	☐	☐
19.7.8.5	Ensure 'Turn off Spotlight collection on Desktop' is set to 'Enabled' (Automated)	☐	☐
19.7.9	Credential User Interface		
19.7.10	Data Collection and Preview Builds		
19.7.11	Desktop Gadgets		
19.7.12	Desktop Window Manager		
19.7.13	Digital Locker		
19.7.14	Edge UI		
19.7.15	File Explorer (formerly Windows Explorer)		
19.7.15.1	Explorer Frame Pane		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
19.7.15.1.1	Ensure 'Turn off Preview Pane' is set to 'Enabled' (Automated)	☐	☐
19.7.15.1.2	Ensure 'Turn on off details pane' is set to 'Enabled: Always hide' (Automated)	☐	☐
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		
19.7.26.1	Ensure 'Prevent users from sharing files within their profile.' is set to 'Enabled' (Automated)	☐	☐
19.7.27	Oobe		
19.7.28	Presentation Settings		
19.7.29	Remote Desktop Services (formerly Terminal Services)		
19.7.30	RSS Feeds		
19.7.31	Search		
19.7.32	Sound Recorder		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
19.7.33	Store		
19.7.34	Tablet PC		
19.7.35	Task Scheduler		
19.7.36	Windows Calendar		
19.7.37	Windows Color System		
19.7.38	Windows Copilot		
19.7.39	Windows Defender SmartScreen		
19.7.40	Windows Error Reporting		
19.7.41	Windows Hello for Business (formerly Microsoft Passport for Work)		
19.7.42	Windows Installer		
19.7.42.1	Ensure 'Always install with elevated privileges' is set to 'Disabled' (Automated)	☐	☐
19.7.43	Windows Logon Options		
19.7.44	Windows Media Player		
19.7.44.1	Networking		
19.7.44.2	Playback		
19.7.44.2.1	Ensure 'Prevent Codec Download' is set to 'Enabled' (Automated)	☐	☐
20	Additional Security Technical Implementation Guide (STIG) Settings		
20.1	Ensure 'Accounts require passwords' (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
20.2	Ensure 'Active Directory AdminSDHolder object is configured with proper audit settings' (STIG DC only) (Manual)	☐	☐
20.3	Ensure 'Active Directory Domain Controllers Organizational Unit (OU) object have the proper access control permissions' (STIG DC only) (Manual)	☐	☐
20.4	Ensure 'Active Directory Domain Controllers Organizational Unit (OU) object is configured with proper audit settings' (STIG DC only) (Manual)	☐	☐
20.5	Ensure 'Active Directory Domain object is configured with proper audit settings' (STIG DC only) (Manual)	☐	☐
20.6	Ensure 'Active Directory Group Policy objects are configured with proper audit settings' (STIG DC only) (Manual)	☐	☐
20.7	Ensure 'Active Directory Group Policy objects have proper access control permissions' (STIG DC only) (Manual)	☐	☐
20.8	Ensure 'Active Directory Infrastructure object is configured with proper audit settings' (STIG DC only) (Manual)	☐	☐
20.9	Ensure 'Active Directory RID Manager\$ object is configured with proper audit settings' (STIG DC only) (Manual)	☐	☐
20.10	Ensure 'Active Directory SYSVOL directory must have the proper access control permissions' (STIG DC only) (Manual)	☐	☐
20.11	Ensure 'Active Directory user accounts are configured to require the use of a Common Access Card (CAC), Personal Identity Verification (PIV)-compliant hardware token, or Alternate Logon Token (ALT)' (STIG DC only) (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
20.12	Ensure 'Administrative accounts cannot be used with applications that access the Internet, such as web browsers, or with potential Internet sources, such as email' (Manual)	☐	☐
20.13	Ensure 'Audit records must be backed up to a different system or media than the system being audited' (Manual)	☐	☐
20.14	Ensure 'Automated mechanisms must be employed to determine the state of system components...' (Manual)	☐	☐
20.15	Ensure 'Data files owned by users must be on a different logical partition from the directory server data files' (STIG DC only) (Manual)	☐	☐
20.16	Ensure 'Default permissions for the HKEY_LOCAL_MACHINE registry hive must be maintained' (Manual)	☐	☐
20.17	Ensure 'Deny-all, permit-by-exception policy to allow the execution of authorized software programs' (Manual)	☐	☐
20.18	Ensure 'Directory data (outside the root DSE) of a non-public directory is configured' (STIG DC only) (Manual)	☐	☐
20.19	Ensure 'Directory service must be configured to terminate LDAP-based network connections to the directory server after five minutes of inactivity' (STIG DC only) (Manual)	☐	☐
20.20	Ensure 'DoD Interoperability Root CA cross-certificates' are installed in the 'Untrusted Certificates Store' on unclassified systems (Manual)	☐	☐
20.21	Ensure 'DoD Root Certificate Authority (CA) certificates' are installed in the 'Trusted Root Store' (Manual)	☐	☐
20.22	Ensure 'Domain Controller PKI certificates must be issued by the DoD PKI or an approved External Certificate Authority' (STIG DC only) (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
20.23	Ensure 'Domain controllers have a PKI server certificate' (STIG DC only) (Manual)	☐	☐
20.24	Ensure 'Domain Controllers run on a machine dedicated to that function' (STIG DC only) (Manual)	☐	☐
20.25	Ensure 'Domain-joined systems have a Trusted Platform Module (TPM) enabled and ready for use' (Manual)	☐	☐
20.26	Ensure 'Emergency accounts must be automatically removed or disabled after the crisis is resolved or within 72 hours' (Manual)	☐	☐
20.27	Ensure 'Event Viewer must be protected from unauthorized modification and deletion' (Manual)	☐	☐
20.28	Ensure 'Fax Server role' is set to 'Not Installed' (Manual)	☐	☐
20.29	Ensure 'FTP servers are configured to prevent access to the system drive' (Manual)	☐	☐
20.30	Ensure 'FTP servers must be configured to prevent anonymous logons' (Manual)	☐	☐
20.31	Ensure 'Host-based firewall is installed and enabled' (Manual)	☐	☐
20.32	Ensure 'krbtgt account password' is no more than '180 days old' (STIG DC only) (Manual)	☐	☐
20.33	Ensure 'Local volumes must use a format that supports NTFS attributes' (Manual)	☐	☐
20.34	Ensure 'Manually managed application account passwords are 14 characters in length' (Manual)	☐	☐
20.35	Ensure 'Manually managed application account passwords be changed at least annually or when a system administrator with knowledge of the password leaves the organization' (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
20.36	Ensure 'Members of the Backup Operators group have separate accounts for backup duties and normal operational tasks' (Manual)	☐	☐
20.37	Ensure 'Non-administrative accounts or groups only have print permissions on printer shares' (Manual)	☐	☐
20.38	Ensure 'Non-system-created file shares must limit access to groups that require it' (Manual)	☐	☐
20.39	Ensure 'Off-load of audit records of interconnected systems in real time and off-load standalone systems weekly' (Manual)	☐	☐
20.40	Ensure 'Only Administrators have Administrator rights on the system' (STIG MS only) (Manual)	☐	☐
20.41	Ensure 'Only administrators responsible for the Domain Controller to have Administrator rights on the system' (STIG DC only) (Manual)	☐	☐
20.42	Ensure 'Operating System is maintained at a supported servicing level' (Manual)	☐	☐
20.43	Ensure 'Organization created Active Directory Organizational Unit (OU) objects have proper access control permissions' (STIG DC only) (Manual)	☐	☐
20.44	Ensure 'Orphaned security identifiers (SIDs) must be removed from user rights' (Manual)	☐	☐
20.45	Ensure 'Outdated or unused accounts are removed or disabled' (Manual)	☐	☐
20.46	Ensure 'Passwords are configured to expire' (Manual)	☐	☐
20.47	Ensure 'Permissions for program file directories must conform to minimum requirements' (Manual)	☐	☐
20.48	Ensure 'Permissions for the Application Event Log must prevent access by non-privileged accounts' (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
20.49	Ensure 'Permissions for the Security Event Log must prevent access by non-privileged accounts' (Manual)	☐	☐
20.50	Ensure 'Permissions for the System Event Log must prevent access by non-privileged accounts' (Manual)	☐	☐
20.51	Ensure 'Permissions for the system drive root directory must conform to minimum requirements' (Manual)	☐	☐
20.52	Ensure 'Permissions for the Windows installation directory conform to minimum requirements' (Manual)	☐	☐
20.53	Ensure 'Permissions on Active Directory data files only allow System and Administrator access' (STIG DC only) (Manual)	☐	☐
20.54	Ensure 'PKI certificates associated with user accounts must be issued by a DoD PKI or an approved External Certificate Authority (ECA)' (STIG DC only) (Manual)	☐	☐
20.55	Ensure 'Protection methods such as TLS, encrypted VPN's, or IPsec must be implemented if the data owner has a strict requirement for ensuring data integrity and confidentiality is maintained at every step of the data transfer and handling process' (Manual)	☐	☐
20.56	Ensure 'Separate NSA-approved (Type 1) cryptography is used' (STIG DC only) (Manual)	☐	☐
20.57	Ensure 'Server Message Block (SMB) v1 protocol must not be installed' (Manual)	☐	☐
20.58	Ensure 'Shared user accounts do not exist' (Manual)	☐	☐
20.59	Ensure 'Software certificate installation files must be removed' (Manual)	☐	☐
20.60	Ensure 'System files must be monitored for unauthorized changes' (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
20.61	Ensure 'Systems requiring data at rest protections must employ cryptographic mechanisms to prevent unauthorized disclosure and modification of the information at rest' (Manual)	☐	☐
20.62	Ensure 'Telnet Client is not installed' (Manual)	☐	☐
20.63	Ensure 'Temporary user accounts must be automatically removed or disabled after 72 hours' (Manual)	☐	☐
20.64	Ensure 'TFTP Client' is 'not installed' (Manual)	☐	☐
20.65	Ensure 'The system must have the Roles and Features required for it documented' (Manual)	☐	☐
20.66	Ensure 'The system uses a host-based intrusion detection or prevention system' (Manual)	☐	☐
20.67	Ensure 'The system uses an anti-virus program' (Manual)	☐	☐
20.68	Ensure 'Unified Extensible Firmware Interface (UEFI) firmware must be configured and run in UEFI mode, not Legacy BIOS' (Manual)	☐	☐
20.69	Ensure 'US DoD CCEB Interoperability Root CA cross-certificates' are installed in the 'Untrusted Certificates Store' on unclassified systems (Manual)	☐	☐
20.70	Ensure 'Users with Administrative privileges have separate accounts for administrative duties and normal operational tasks' (Manual)	☐	☐
20.71	Ensure 'Windows PowerShell 2.0' is 'not installed' (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
9/15/2020	1.0.0	Initial Public Release
7/30/2021	1.1.0	UPDATE - 1.1.2 (L1) Ensure 'Maximum password age' is set to '60 or fewer days, but not 0' TO '365 or fewer days, but not 0' to match updated CIS Password Policy recommendations Ticket #12627
7/30/2021	1.1.0	ADD - Section changes from Windows 10 Release 21H1 Administrative Templates Ticket #12970
7/30/2021	1.1.0	UPDATE - 1.2.2 (L1) Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0' TO '5 or fewer invalid logon attempt(s), but not 0' Ticket #13188
04/21/2022	1.4.0	REMOVE - 19.1.3 (L1) Ensure 'Force specific screen saver: Screen saver executable name' is set to 'Enabled: scrnsave.scr' Ticket #8782
04/21/2022	1.2.0	ADD - 5 (L1) Ensure 'Print Spooler (Spooler)' is set to 'Disabled' (DC only) Ticket# 13338
04/21/2022	1.2.0	ADD - 5 (L2) Ensure 'Print Spooler (Spooler)' is set to 'Disabled' (MS only) Ticket# 13339
04/21/2022	1.2.0	ADD - 18.6 (L1) Ensure 'Point and Print Restrictions: When installing drivers for a new connection' is set to 'Enabled: Show warning and elevation prompt' Ticket# 13340

Date	Version	Changes for this version
04/21/2022	1.2.0	ADD - 18.6 (L1) Ensure 'Point and Print Restrictions: When updating drivers for an existing connection' is set to 'Enabled: Show warning and elevation prompt' Ticket# 13341
04/21/2022	1.2.0	ADD - 18.6 (L1) Ensure 'Allow Print Spooler to accept client connections' is set to 'Disabled' Ticket# 13343
04/21/2022	1.2.0	ADD - 18.8.7 (L1) Ensure 'Prevent device metadata retrieval from the Internet' is set to 'Enabled' Ticket# 13759
04/21/2022	1.2.0	ADD - Section changes from Windows 11 Release 21H2 Administrative Templates Ticket# 13968
04/21/2022	1.2.0	RENAME - 9 Windows Firewall with Advanced Security TO Windows Defender Firewall with Advanced Security Ticket# 14034
04/21/2022	1.2.0	RENAME & UPDATE - 18.9.17 (L1) Ensure 'Allow Telemetry' TO (L1) Ensure 'Allow Diagnostic Data' Ticket# 14035
04/21/2022	1.2.0	MOVE - 18.9.103 (L1) Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled' TO 18.9.108.1 Legacy Policies Ticket# 14043
04/21/2022	1.2.0	MOVE - 18.9.103 (L1) Ensure 'Configure Automatic Updates' is set to 'Enabled' TO 18.9.108.2 Manage end user experience Ticket# 14044
04/21/2022	1.2.0	MOVE - 18.9.103 (L1) Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day' TO 18.9.108.2 Manage end user experience Ticket# 14045

Date	Version	Changes for this version
04/21/2022	1.2.0	MOVE & UPDATE - 18.9.103.1 (L1) Ensure 'Manage preview builds' is set to 'Enabled: Disable preview builds' TO 18.9.108.4 (L1) Ensure 'Manage preview builds' is set to 'Disabled' Ticket# 14050
04/21/2022	1.2.0	MOVE & UPDATE - 18.9.103.1 (L1) Ensure 'Select when Preview Builds and Feature Updates are received' is set to 'Enabled: Semi-Annual Channel, 180 or more days' TO 18.9.108.4 'Enabled: 180 or more days' Ticket# 14051
04/21/2022	1.2.0	ADD - 18.3 (L1) Ensure 'Limits print driver installation to Administrators' is set to 'Enabled' Ticket# 14578
04/21/2022	1.2.0	ADD - 18.5.4 (L1) Ensure 'Configure DNS over HTTPS (DoH) name resolution' is set to 'Enabled: Allow DoH' or higher Ticket# 14579
04/21/2022	1.2.0	ADD - 18.8.40 (L1) Ensure 'Configure validation of ROCA-vulnerable WHfB keys during authentication' is set to 'Enabled: Audit' or higher (DC only) Ticket# 14580
04/21/2022	1.2.0	ADD - 18.9.14 (L1) Ensure 'Turn off cloud consumer account state content' is set to 'Enabled' Ticket# 14581
04/21/2022	1.2.0	ADD - 18.9.17 (L1) Ensure 'Enable OneSettings Auditing' is set to 'Enabled' Ticket# 14582
04/21/2022	1.2.0	ADD - 18.9.17 (L1) Ensure 'Limit Diagnostic Log Collection' is set to 'Enabled' Ticket# 14583

Date	Version	Changes for this version
04/21/2022	1.2.0	ADD - 18.9.17 (L1) Ensure 'Limit Dump Collection' is set to 'Enabled' Ticket# 14584
04/21/2022	1.2.0	ADD - 18.9.47.9 (L1) Ensure 'Turn on script scanning' is set to 'Enabled' Ticket# 14585
04/21/2022	1.2.0	ADD - 19.7.8 (L1) Ensure 'Turn off Spotlight collection on Desktop' is set to 'Enabled' Ticket# 14588
04/21/2022	1.2.0	ADD - 18.9.17 (L1) Ensure 'Disable OneSettings Downloads' is set to 'Enabled' Ticket# 14625
04/21/2022	1.2.0	UPDATE - 18.9.100 (L1) Ensure 'Turn on PowerShell Script Block Logging' is set to 'Disabled' TO 'Enabled' Ticket# 14637
04/21/2022	1.2.0	UPDATE - 18.8.3 (L1) Ensure 'Include command line in process creation events' is set to 'Disabled' TO 'Enabled' Ticket# 14638
10/20/2023	2.0.0	REMOVE - 18.5.4 (L1) Ensure 'Configure DNS over HTTPS (DoH) name resolution' is set to 'Enabled: Allow DoH' or higher Ticket# 15653
10/20/2023	2.0.0	UPDATE - 18.9.89 'Allow Windows Ink Workspace' TO 'Enabled: On, but disallow access above lock' OR 'Enabled: Disabled' Ticket# 16103
10/20/2023	2.0.0	ADD - 18.9.47.5.1 'Configure Attack Surface Reduction rules' is set to 'Enable' Ticket# 17076

Date	Version	Changes for this version
10/20/2023	2.0.0	UPDATE - Section changes from Windows 11 Release 22H2 Administrative Templates Ticket# 17124
10/20/2023	2.0.0	UPDATE – 18.10.87 (L1) 'Turn on PowerShell Transcription' is set to 'Disabled' TO 'Enabled' Ticket# 17516
10/20/2023	2.0.0	ADD - 1.2 (L1) Ensure 'Allow Administrator account lockout' is set to 'Enabled' Ticket# 17564
10/20/2023	2.0.0	REMOVE - 2.3.1 (L1) Ensure 'Accounts: Administrator account status' is set to 'Disabled' Ticket# 17565
10/20/2023	2.0.0	ADD - 18.4 (L1) Ensure 'Configure RPC packet level privacy setting for incoming connections' is set to 'Enabled' Ticket# 17566
10/20/2023	2.0.0	MOVE - 18.4 (L1) Ensure 'Limits print driver installation to Administrators' is set to 'Enabled' TO 18.7 Ticket# 17567
10/20/2023	2.0.0	ADD - 18.4 (L1) Ensure 'LSA Protection' is set to 'Enabled' Ticket# 17568
10/20/2023	2.0.0	ADD - 18.6.4 (L1) Ensure 'Configure NetBIOS settings' is set to 'Enabled: Disable NetBIOS name resolution on public networks' Ticket# 17569
10/20/2023	2.0.0	ADD - 18.7 (L1) Ensure 'Configure Redirection Guard' is set to 'Enabled: Redirection Guard Enabled' Ticket# 17570

Date	Version	Changes for this version
10/20/2023	2.0.0	ADD - 18.7 (L1) Ensure 'Configure RPC connection settings: Protocol to use for outgoing RPC connections' is set to 'Enabled: RPC over TCP' Ticke # 17572
10/20/2023	2.0.0	ADD - 18.7 (L1) Ensure 'Configure RPC connection settings: Use authentication for outgoing RPC connections' is set to 'Enabled: Default' Ticket# 17573
10/20/2023	2.0.0	ADD - 18.7 (L1) Ensure 'Configure RPC listener settings: Protocols to allow for incoming RPC connections' is set to 'Enabled: RPC over TCP' Ticket# 17575
10/20/2023	2.0.0	ADD - 18.7 (L1) Ensure 'Configure RPC listener settings: Authentication protocol to use for incoming RPC connections' is set to 'Enabled: Negotiate' or higher Ticket# 17576
10/20/2023	2.0.0	ADD - 18.7 (L1) Ensure 'Manage processing of Queue-specific files' is set to 'Enabled: Limit Queue-specific files to Color profiles' Ticket# 17577
10/20/2023	2.0.0	UPDATE - 18.10.43.6.1 (L1) Ensure 'Configure Attack Surface Reduction rules' with additional ASR rule for "Block abuse of exploited vulnerable signed drivers" Ticket# 17588
10/20/2023	2.0.0	ADD - 18.10.59 (L2) Ensure 'Allow search highlights' is set to 'Disabled' Ticket# 17591
10/20/2023	2.0.0	ADD - 18.7 (L1) Ensure 'Configure RPC over TCP port' is set to 'Enabled: 0' Ticket# 17715

Date	Version	Changes for this version
10/20/2023	2.0.0	UPDATE - 9 Windows Firewall with Advanced Security TO Windows Defender Firewall with Advanced Security Ticket #18532
10/20/2023	2.0.0	UPDATE - 2016 STIG 17.4 (L1) Ensure 'Audit Directory Service Changes' is set to include 'Success' and 'Failure TO 'Success' Ticket #20003
10/20/2023	2.0.0	UPDATE - 2016 STIG 18.9.13.2 (L1) Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good, unknown and bad but critical' TO 'Enabled: any, but ALL' Ticket #20004
10/20/2023	2.0.0	REMOVE - 2016 STIG 18.4.1 (L1) Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled' (MS only) Ticket #20006
10/20/2023	2.0.0	REMOVE - 2016 STIG 20.21 Ensure 'DoD Root Certificate Authority (CA) certificates' are installed in the 'Trusted Root Store' Ticket #20007
10/20/2023	2.0.0	REMOVE - 2016 STIG 20.69 Ensure 'US DoD CCEB Interoperability Root CA cross-certificates' are installed in the 'Untrusted Certificates Store' on unclassified systems Ticket #20008
08/26/2024	3.0.0	UPDATE - 18.9.50.1 (L2 -> L1) Ensure 'Enable Windows NTP Client' is set to 'Enabled' Ticket #18467
08/26/2024	3.0.0	UPDATE - 18.9.50.1 (L2 -> L1) Ensure 'Enable Windows NTP Server' is set to 'Disabled' Ticket #18468

Date	Version	Changes for this version
08/26/2024	3.0.0	UPDATE - 9 Windows Firewall with Advanced Security TO Windows Defender Firewall with Advanced Security Ticket #18532
08/26/2024	3.0.0	UPDATE - 18.10.42.7 (L2 -> L1) Ensure 'Enable file hash computation feature' is set to 'Enabled' Ticket #19207
08/26/2024	3.0.0	ADD - 18.9.19 (L1) 'Configure security policy processing: Do not apply during periodic background processing' is set to 'False' Ticket #19358
08/26/2024	3.0.0	ADD - 18.9.19 (L1) 'Configure security policy processing: Process even if the Group Policy objects have not changed' is set to 'True' Ticket #19359
08/26/2024	3.0.0	REMOVE - 19.1.3 Accepted (L1) Ensure 'Password protect the screen saver' is set to 'Enabled' Ticket #19361
08/26/2024	3.0.0	REMOVE - 19.1.3 Accepted (L1) Ensure 'Screen saver timeout' is set to 'Enabled: 900 seconds or fewer, but not 0' Ticket #19362
08/26/2024	3.0.0	REMOVE - 18.9.38 (L1) Ensure 'Configure validation of ROCA-vulnerable WHfB keys during authentication' is set to 'Enabled: Audit' or higher (DC only) Ticket #19697
08/26/2024	3.0.0	ADD - 2.3.11 (L1) Ensure 'Network security: Restrict NTLM: Audit Incoming NTLM Traffic' is set to 'Enable auditing for all accounts' Ticket #19740

Date	Version	Changes for this version
08/26/2024	3.0.0	ADD - 2.3.11 (L1) Ensure 'Network security: Restrict NTLM: Audit NTLM authentication in this domain' is set to 'Enable all' (DC only) Ticket #19741
08/26/2024	3.0.0	ADD - 2.3.11 (L1) Ensure 'Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers' is set to 'Audit all' or higher Ticket #19742
08/26/2024	3.0.0	REMOVE - 2.3.4 (L1) Ensure 'Devices: Allowed to format and eject removable media' is set Ticket #20103
08/26/2024	3.0.0	UPDATE - Section changes from Windows 11 Release 22H2 v3.0 Administrative Templates Ticket #20220
08/26/2024	3.0.0	UPDATE - Section changes from Windows 11 Release 23H2 Administrative Templates Ticket #20324
08/26/2024	3.0.0	ADD - 18.10.42.13 (L1) Ensure 'Scan packed executables' is set to 'Enabled' Ticket #20337
08/26/2024	3.0.0	UPDATE - 2.2 (L1) Ensure 'Allow log on locally' is set to 'Administrators' TO 'Administrators, ENTERPRISE DOMAIN CONTROLLERS' (DC only) Ticket #20339
08/26/2024	3.0.0	UPDATE - 18.5 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' TO 'MSS: (AutoAdminLogon) Enable Automatic Logon' Ticket #20355

Date	Version	Changes for this version
08/26/2024	3.0.0	UPDATE - 18.5 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' TO 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level' Ticket #20357
08/26/2024	3.0.0	UPDATE - 18.5 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' TO 'MSS: (DisableIPSourceRouting) IP source routing protection level' Ticket #20358
08/26/2024	3.0.0	UPDATE - 18.5 'MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)' TO 'MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses' Ticket #20359
08/26/2024	3.0.0	UPDATE - 18.5 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' TO 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode' Ticket #20360
08/26/2024	3.0.0	UPDATE - 18.5 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)' TO 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires' Ticket #20361
08/26/2024	3.0.0	UPDATE - 18.5 'MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds' is set to 'Enabled: 300,000 or 5 minutes (recommended)' TO 'Enabled: 300,000 or 5 minutes' Ticket #20362
08/26/2024	3.0.0	REMOVE - 18.10.24 EMET Ticket #20472

Date	Version	Changes for this version
08/26/2024	3.0.0	ADD - 18.4 (L1) Ensure 'Enable Certificate Padding' is set to 'Enabled' Ticket #20521
08/26/2024	3.0.0	REMOVE - 9.1 (L1) Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)' Ticket #20526
08/26/2024	3.0.0	REMOVE - 9.2 (L1) Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)' Ticket #20527
08/26/2024	3.0.0	REMOVE - 9.3 (L1) Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)' Ticket #20528
08/26/2024	3.0.0	REMOVE - 19.1.3 (L1) Ensure 'Enable screen saver' is set to 'Enabled' Ticket #20634
08/26/2024	3.0.0	UPDATE - 18.10.86 (L1 -> L2) Ensure 'Turn on PowerShell Script Block Logging' is set to 'Enabled' Ticket #20717
08/26/2024	3.0.0	UPDATE - 18.10.86 (L1 -> L2) Ensure 'Turn on PowerShell Transcription' is set to 'Enabled' Ticket #20718
08/26/2024	3.0.0	UPDATE - 18.6.14 (L1) Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" for all NETLOGON and SYSVOL shares' TO add "Require Privacy" Ticket #20785
08/26/2024	3.0.0	UPDATE - Section 17 Auditpol commands Ticket #21446

Date	Version	Changes for this version
08/26/2024	3.0.0	UPDATE - 2.2 Ensure 'Deny log on as a service' to include 'No one' (STIG DC only) Ticket #21984
08/26/2024	3.0.0	UPDATE - 18.10.75.2 Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled' (STIG only) Ticket #21994
08/26/2024	3.0.0	UPDATE - 2.3.17 Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop' (STIG only) TO 'Prompt for consent on the secure desktop' or higher Ticket #21996
08/26/2024	3.0.0	UPDATE - Firewall UI path Ticket #22051
08/26/2024	3.0.0	REMOVE - 17.5 Ensure 'Audit Account Lockout' is set to include 'Success and Failure' (STIG only) Ticket #22260
08/26/2024	3.0.0	ADD - 17.6 Ensure 'Audit Removable Storage' is set to 'Success and Failure' Ticket #22261
08/26/2024	3.0.0	UPDATE - 20 Ensure 'DoD Interoperability Root CA cross-certificates' are installed in the 'Untrusted Certificates Store' on unclassified systems Ticket #22262
08/26/2024	3.0.0	UPDATE - 20 Ensure 'Manually managed application account passwords are 15 characters in length' TO Ensure 'Manually managed application account passwords are 14 characters in length' Ticket #22263

Date	Version	Changes for this version
08/26/2024	3.0.0	ADD - 18.10.86 Ensure 'Turn on PowerShell Transcription' is set to 'Enabled' Ticket #22264
08/26/2024	3.0.0	ADD - 18.4 Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled' Ticket #22265
08/26/2024	3.0.0	ADD - 20 Ensure 'DoD Root Certificate Authority (CA) certificates' are installed in the 'Trusted Root Store' Ticket #22291
08/26/2024	3.0.0	ADD - 20 Ensure 'US DoD CCEB Interoperability Root CA cross-certificates' are installed in the 'Untrusted Certificates Store' on unclassified systems Ticket #22292