CIS Benchmarks

CIS Microsoft Windows Server 2012 (non-R2) Benchmark

v2.2.0 - 04-28-2020

Terms of Use

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

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

Table of Contents

Terms of Use 1

Overview 33

Intended Audience 33

Consensus Guidance 33

Typographical Conventions 34

Scoring Information 34

Profile Definitions 35

Acknowledgements 37

Recommendations 38

1 Account Policies 38

1.1 Password Policy 38

1.1.1 (L1) Ensure 'Enforce password history' is set to '24 or more password(s)' (Scored) 38

1.1.2 (L1) Ensure 'Maximum password age' is set to '60 or fewer days, but not 0' (Scored) 41

1.1.3 (L1) Ensure 'Minimum password age' is set to '1 or more day(s)' (Scored) 43

1.1.4 (L1) Ensure 'Minimum password length' is set to '14 or more character(s)' (Scored) 45

1.1.5 (L1) Ensure 'Password must meet complexity requirements' is set to 'Enabled' (Scored) 48

1.1.6 (L1) Ensure 'Store passwords using reversible encryption' is set to 'Disabled' (Scored) 51

1.2 Account Lockout Policy 53

1.2.1 (L1) Ensure 'Account lockout duration' is set to '15 or more minute(s)' (Scored) 53

1.2.2 (L1) Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0' (Scored) 55

1.2.3 (L1) Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)' (Scored) 57

2 Local Policies 60

2.1 Audit Policy 60
2.2 User Rights Assignment 61
2.2.1 (L1) Ensure 'Access Credential Manager as a trusted caller' is set to 'No One' (Scored) 61
2.2.2 (L1) Ensure 'Access this computer from the network' is set to 'Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS' (DC only) (Scored) 63
2.2.3 (L1) Ensure 'Access this computer from the network' is set to 'Administrators, Authenticated Users' (MS only) (Scored) 65
2.2.4 (L1) Ensure 'Act as part of the operating system' is set to 'No One' (Scored) 67
2.2.5 (L1) Ensure 'Add workstations to domain' is set to 'Administrators' (DC only) (Scored) 69
2.2.6 (L1) Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE' (Scored) 72
2.2.7 (L1) Ensure 'Allow log on locally' is set to 'Administrators' (Scored) 75
2.2.8 (L1) Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators' (DC only) (Scored) 77
2.2.9 (L1) Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators, Remote Desktop Users' (MS only) (Scored) 80
2.2.10 (L1) Ensure 'Back up files and directories' is set to 'Administrators' (Scored) 83
2.2.11 (L1) Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE' (Scored) 85
2.2.12 (L1) Ensure 'Change the time zone' is set to 'Administrators, LOCAL SERVICE' (Scored) 88
2.2.13 (L1) Ensure 'Create a pagefile' is set to 'Administrators' (Scored) 90
2.2.14 (L1) Ensure 'Create a token object' is set to 'No One' (Scored) 92
2.2.15 (L1) Ensure 'Create global objects' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (Scored) 94
2.2.16 (L1) Ensure 'Create permanent shared objects' is set to 'No One' (Scored) 96
2.2.17 (L1) Ensure 'Create symbolic links' is set to 'Administrators' (DC only) (Scored) 98

2.2.18 (L1) Ensure 'Create symbolic links' is set to 'Administrators, NT VIRTUAL MACHINE\Virtual Machines' (MS only) (Scored) 100

2.2.19 (L1) Ensure 'Debug programs' is set to 'Administrators' (Scored) 102

2.2.20 (L1) Ensure 'Deny access to this computer from the network' to include 'Guests' (DC only) (Scored) 105

2.2.21 (L1) Ensure 'Deny access to this computer from the network' to include 'Guests, Local account and member of Administrators group' (MS only) (Scored) 107

2.2.22 (L1) Ensure 'Deny log on as a batch job' to include 'Guests' (Scored) 109

2.2.23 (L1) Ensure 'Deny log on as a service' to include 'Guests' (Scored) 111

2.2.24 (L1) Ensure 'Deny log on locally' to include 'Guests' (Scored) 113

2.2.25 (L1) Ensure 'Deny log on through Remote Desktop Services' to include 'Guests' (DC only) (Scored) 115

2.2.26 (L1) Ensure 'Deny log on through Remote Desktop Services' is set to 'Guests, Local account' (MS only) (Scored) 117

2.2.27 (L1) Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'Administrators' (DC only) (Scored) 119

2.2.28 (L1) Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'No One' (MS only) (Scored) 121

2.2.29 (L1) Ensure 'Force shutdown from a remote system' is set to 'Administrators' (Scored) 123

2.2.30 (L1) Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE' (Scored) 125

2.2.31 (L1) Ensure 'Impersonate a client after authentication' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (DC only) (Scored) 127

2.2.32 (L1) 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) (Scored) 130

2.2.33 (L1) Ensure 'Increase scheduling priority' is set to 'Administrators' (Scored) 133

2.2.34 (L1) Ensure 'Load and unload device drivers' is set to 'Administrators' (Scored) 135

2.2.35 (L1) Ensure 'Lock pages in memory' is set to 'No One' (Scored) 137
2.2.36 (L2) Ensure 'Log on as a batch job' is set to 'Administrators' (DC Only) (Scored) 139
2.2.37 (L1) Ensure 'Manage auditing and security log' is set to 'Administrators' and (when Exchange is running in the environment) 'Exchange Servers' (DC only) (Scored) 141
2.2.38 (L1) Ensure 'Manage auditing and security log' is set to 'Administrators' (MS only) (Scored) 143
2.2.39 (L1) Ensure 'Modify an object label' is set to 'No One' (Scored) 145
2.2.40 (L1) Ensure 'Modify firmware environment values' is set to 'Administrators' (Scored) 147
2.2.41 (L1) Ensure 'Perform volume maintenance tasks' is set to 'Administrators' (Scored) 149
2.2.42 (L1) Ensure 'Profile single process' is set to 'Administrators' (Scored) 151
2.2.43 (L1) Ensure 'Profile system performance' is set to 'Administrators, NT SERVICE\WdiServiceHost' (Scored) 153
2.2.44 (L1) Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE' (Scored) 155
2.2.45 (L1) Ensure 'Restore files and directories' is set to 'Administrators' (Scored) 157
2.2.46 (L1) Ensure 'Shut down the system' is set to 'Administrators' (Scored) .. 159
2.2.47 (L1) Ensure 'Synchronize directory service data' is set to 'No One' (DC only) (Scored) 161
2.2.48 (L1) Ensure 'Take ownership of files or other objects' is set to 'Administrators' (Scored) 163
2.3 Security Options 165
2.3.1 Accounts 165
2.3.1.1 (L1) Ensure 'Accounts: Administrator account status' is set to 'Disabled' (MS only) (Scored) 165
2.3.1.2 (L1) Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts' (Scored) 168
2.3.1.3 (L1) Ensure 'Accounts: Guest account status' is set to 'Disabled' (MS only) (Scored) 170

2.3.1.4 (L1) Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled' (Scored) 172
2.3.1.5 (L1) Configure 'Accounts: Rename administrator account' (Scored) 174
2.3.1.6 (L1) Configure 'Accounts: Rename guest account' (Scored) 176
2.3.2 Audit 178
2.3.2.1 (L1) Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled' (Scored) 178
2.3.2.2 (L1) Ensure 'Audit: Shut down system immediately if unable to log security audits' is set to 'Disabled' (Scored) 181
2.3.3 DCOM 183
2.3.4 Devices 184
2.3.4.1 (L1) Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators' (Scored) 184
2.3.4.2 (L1) Ensure 'Devices: Prevent users from installing printer drivers' is set to 'Enabled' (Scored) 187
2.3.5 Domain controller 189
2.3.5.1 (L1) Ensure 'Domain controller: Allow server operators to schedule tasks' is set to 'Disabled' (DC only) (Scored) 189
2.3.5.2 (L1) Ensure 'Domain controller: LDAP server signing requirements' is set to 'Require signing' (DC only) (Scored) 191
2.3.5.3 (L1) Ensure 'Domain controller: Refuse machine account password changes' is set to 'Disabled' (DC only) (Scored) 194
2.3.6 Domain member 196
2.3.6.1 (L1) Ensure 'Domain member: Digitally encrypt or sign secure channel data (always)' is set to 'Enabled' (Scored) 196
2.3.6.2 (L1) Ensure 'Domain member: Digitally encrypt secure channel data (when possible)' is set to 'Enabled' (Scored) 199
2.3.6.3 (L1) Ensure 'Domain member: Digitally sign secure channel data (when possible)' is set to 'Enabled' (Scored) 201
2.3.6.4 (L1) Ensure 'Domain member: Disable machine account password changes' is set to 'Disabled' (Scored) 203
2.3.6.5 (L1) Ensure 'Domain member: Maximum machine account password age' is set to '30 or fewer days, but not 0' (Scored) 205

2.3.6.6 (L1) Ensure 'Domain member: Require strong (Windows 2000 or later) session key' is set to 'Enabled' (Scored) 207
2.3.7 Interactive logon 209
2.3.7.1 (L1) Ensure 'Interactive logon: Do not display last user name' is set to 'Enabled' (Scored) 209
2.3.7.2 (L1) Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled' (Scored) 211
2.3.7.3 (L1) Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0' (Scored) 213
2.3.7.4 (L1) Configure 'Interactive logon: Message text for users attempting to log on' (Scored) 215
2.3.7.5 (L1) Configure 'Interactive logon: Message title for users attempting to log on' (Scored) 217
2.3.7.6 (L2) Ensure 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' is set to '4 or fewer logon(s)' (MS only) (Scored) 219
2.3.7.7 (L1) Ensure 'Interactive logon: Prompt user to change password before expiration' is set to 'between 5 and 14 days' (Scored) 222
2.3.7.8 (L1) Ensure 'Interactive logon: Require Domain Controller Authentication to unlock workstation' is set to 'Enabled' (MS only) (Scored) 224
2.3.7.9 (L1) Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher (Scored) 226
2.3.8 Microsoft network client 228
2.3.8.1 (L1) Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled' (Scored) 228
2.3.8.2 (L1) Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled' (Scored) 231
2.3.8.3 (L1) Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled' (Scored) 234
2.3.9 Microsoft network server 236
2.3.9.1 (L1) Ensure 'Microsoft network server: Amount of idle time required before suspending session' is set to '15 or fewer minute(s)' (Scored) 236
2.3.9.2 (L1) Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled' (Scored) 238

2.3.9.3 (L1) Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled' (Scored) 241

2.3.9.4 (L1) Ensure 'Microsoft network server: Disconnect clients when logon hours expire' is set to 'Enabled' (Scored) 244

2.3.9.5 (L1) Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher (MS only) (Scored) 246

2.3.10 Network access 249

2.3.10.1 (L1) Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled' (Scored) 249

2.3.10.2 (L1) Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled' (MS only) (Scored) 251

2.3.10.3 (L1) Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled' (MS only) (Scored) 253

2.3.10.4 (L2) Ensure 'Network access: Do not allow storage of passwords and credentials for network authentication' is set to 'Enabled' (Scored) 255

2.3.10.5 (L1) Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled' (Scored) 257

2.3.10.6 (L1) Configure 'Network access: Named Pipes that can be accessed anonymously' (DC only) (Scored) 259

2.3.10.7 (L1) Configure 'Network access: Named Pipes that can be accessed anonymously' (MS only) (Scored) 261

2.3.10.8 (L1) Configure 'Network access: Remotely accessible registry paths' (Scored) 263

2.3.10.9 (L1) Configure 'Network access: Remotely accessible registry paths and sub-paths' (Scored) 266

2.3.10.10 (L1) Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled' (Scored) 270

2.3.10.11 (L1) Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None' (Scored) 273

2.3.10.12 (L1) Ensure 'Network access: Sharing and security model for local accounts' is set to 'Classic - local users authenticate as themselves' (Scored) 275

2.3.11 Network security 277

2.3.11.1 (L1) Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled' (Scored) 277

2.3.11.2 (L1) Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled' (Scored) 279

2.3.11.3 (L1) Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled' (Scored) 281

2.3.11.4 (L1) Ensure 'Network security: Configure encryption types allowed for Kerberos' is set to 'AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types' (Scored) 283

2.3.11.5 (L1) Ensure 'Network security: Do not store LAN Manager hash value on next password change' is set to 'Enabled' (Scored) 285

2.3.11.6 (L1) Ensure 'Network security: Force logoff when logon hours expire' is set to 'Enabled' (Not Scored) 287

2.3.11.7 (L1) Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM' (Scored) 289

2.3.11.8 (L1) Ensure 'Network security: LDAP client signing requirements' is set to 'Negotiate signing' or higher (Scored) 292

2.3.11.9 (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit encryption' (Scored) 294

2.3.11.10 (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption' (Scored) 296

2.3.12 Recovery console 298

2.3.13 Shutdown 299

2.3.13.1 (L1) Ensure 'Shutdown: Allow system to be shut down without having to log on' is set to 'Disabled' (Scored) 299

2.3.14 System cryptography 301

2.3.15 System objects 302

2.3.15.1 (L1) Ensure 'System objects: Require case insensitivity for non-Windows subsystems' is set to 'Enabled' (Scored) 302

2.3.15.2 (L1) Ensure 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)' is set to 'Enabled' (Scored) 304

2.3.16 System settings 306

2.3.16.1 (L1) Ensure 'System settings: Optional subsystems' is set to 'Defined: (blank)' (Scored) 306

2.3.17 User Account Control 308
2.3.17.1 (L1) Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled' (Scored) 308
2.3.17.2 (L1) Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop' (Scored) 310
2.3.17.3 (L1) Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests' (Scored) 312
2.3.17.4 (L1) Ensure 'User Account Control: Detect application installations and prompt for elevation' is set to 'Enabled' (Scored) 314
2.3.17.5 (L1) Ensure 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' is set to 'Enabled' (Scored) 316
2.3.17.6 (L1) Ensure 'User Account Control: Run all administrators in Admin Approval Mode' is set to 'Enabled' (Scored) 318
2.3.17.7 (L1) Ensure 'User Account Control: Switch to the secure desktop when prompting for elevation' is set to 'Enabled' (Scored) 320
2.3.17.8 (L1) Ensure 'User Account Control: Virtualize file and registry write failures to per-user locations' is set to 'Enabled' (Scored) 322
3 Event Log 324
4 Restricted Groups 324
5 System Services 324
6 Registry 324
7 File System 324
8 Wired Network (IEEE 802.3) Policies 324
9 Windows Firewall with Advanced Security 324
9.1 Domain Profile 325
9.1.1 (L1) Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)' (Scored) 325
9.1.2 (L1) Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)' (Scored) 327
9.1.3 (L1) Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)' (Scored) 329
9.1.4 (L1) Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No' (Scored) 331

9.1.5 (L1) Ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\domainfw.log' (Scored) 333
9.1.6 (L1) Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater' (Scored) 335
9.1.7 (L1) Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes' (Scored) 337
9.1.8 (L1) Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes' (Scored) 339
9.2 Private Profile 341
9.2.1 (L1) Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)' (Scored) 341
9.2.2 (L1) Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)' (Scored) 343
9.2.3 (L1) Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)' (Scored) 345
9.2.4 (L1) Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No' (Scored) 347
9.2.5 (L1) Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\privatefw.log' (Scored) 349
9.2.6 (L1) Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater' (Scored) 351
9.2.7 (L1) Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes' (Scored) 353
9.2.8 (L1) Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes' (Scored) 355
9.3 Public Profile 357
9.3.1 (L1) Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)' (Scored) 357
9.3.2 (L1) Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)' (Scored) 359
9.3.3 (L1) Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)' (Scored) 361
9.3.4 (L1) Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'No' (Scored) 363

9.3.5 (L1) Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No' (Scored) 365
9.3.6 (L1) Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No' (Scored) 367
9.3.7 (L1) Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\publicfw.log' (Scored) 369
9.3.8 (L1) Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater' (Scored) 371
9.3.9 (L1) Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes' (Scored) 373
9.3.10 (L1) Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes' (Scored) 375
10 Network List Manager Policies 377
11 Wireless Network (IEEE 802.11) Policies 377
12 Public Key Policies 377
13 Software Restriction Policies 377
14 Network Access Protection NAP Client Configuration 377
15 Application Control Policies 377
16 IP Security Policies 377
17 Advanced Audit Policy Configuration 378
17.1 Account Logon 378
17.1.1 (L1) Ensure 'Audit Credential Validation' is set to 'Success and Failure' (Scored) 378
17.1.2 (L1) Ensure 'Audit Kerberos Authentication Service' is set to 'Success and Failure' (DC Only) (Scored) 381
17.1.3 (L1) Ensure 'Audit Kerberos Service Ticket Operations' is set to 'Success and Failure' (DC Only) (Scored) 383
17.2 Account Management 385
17.2.1 (L1) Ensure 'Audit Application Group Management' is set to 'Success and Failure' (Scored) 385
17.2.2 (L1) Ensure 'Audit Computer Account Management' is set to include 'Success' (DC only) (Scored) 387

17.2.3 (L1) Ensure 'Audit Distribution Group Management' is set to include 'Success' (DC only) (Scored) 389
17.2.4 (L1) Ensure 'Audit Other Account Management Events' is set to include 'Success' (DC only) (Scored) 391
17.2.5 (L1) Ensure 'Audit Security Group Management' is set to include 'Success' (Scored) 393
17.2.6 (L1) Ensure 'Audit User Account Management' is set to 'Success and Failure' (Scored) 395
17.3 Detailed Tracking 397
17.3.1 (L1) Ensure 'Audit Process Creation' is set to include 'Success' (Scored) 397
17.4 DS Access 399
17.4.1 (L1) Ensure 'Audit Directory Service Access' is set to include 'Failure' (DC only) (Scored) 399
17.4.2 (L1) Ensure 'Audit Directory Service Changes' is set to include 'Success' (DC only) (Scored) 401
17.5 Logon/Logoff 403
17.5.1 (L1) Ensure 'Audit Account Lockout' is set to include 'Failure' (Scored) . 403
17.5.2 (L1) Ensure 'Audit Logoff' is set to include 'Success' (Scored) 405
17.5.3 (L1) Ensure 'Audit Logon' is set to 'Success and Failure' (Scored) 407
17.5.4 (L1) Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure' (Scored) 409
17.5.5 (L1) Ensure 'Audit Special Logon' is set to include 'Success' (Scored) 412
17.6 Object Access 414
17.6.1 (L1) Ensure 'Audit Detailed File Share' is set to include 'Failure' (Scored) 414
17.6.2 (L1) Ensure 'Audit File Share' is set to 'Success and Failure' (Scored) 416
17.6.3 (L1) Ensure 'Audit Other Object Access Events' is set to 'Success and Failure' (Scored) 418
17.6.4 (L1) Ensure 'Audit Removable Storage' is set to 'Success and Failure' (Scored) 420
17.7 Policy Change 423
17.7.1 (L1) Ensure 'Audit Audit Policy Change' is set to include 'Success' (Scored) 423

17.7.2 (L1) Ensure 'Audit Authentication Policy Change' is set to include 'Success' (Scored) 426
17.7.3 (L1) Ensure 'Audit Authorization Policy Change' is set to include 'Success' (Scored) 429
17.7.4 (L1) Ensure 'Audit MPSSVC Rule-Level Policy Change' is set to 'Success and Failure' (Scored) 432
17.7.5 (L1) Ensure 'Audit Other Policy Change Events' is set to include 'Failure' (Scored) 434
17.8 Privilege Use 436
17.8.1 (L1) Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure' (Scored) 436
17.9 System 439
17.9.1 (L1) Ensure 'Audit IPsec Driver' is set to 'Success and Failure' (Scored) . 439
17.9.2 (L1) Ensure 'Audit Other System Events' is set to 'Success and Failure' (Scored) 442
17.9.3 (L1) Ensure 'Audit Security State Change' is set to include 'Success' (Scored) 445
17.9.4 (L1) Ensure 'Audit Security System Extension' is set to include 'Success' (Scored) 447
17.9.5 (L1) Ensure 'Audit System Integrity' is set to 'Success and Failure' (Scored) 449
18 Administrative Templates (Computer) 452
18.1 Control Panel 452
18.2 LAPS 453
18.2.1 (L1) Ensure LAPS AdmPwd GPO Extension / CSE is installed (MS only) (Scored) 453
18.2.2 (L1) Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled' (MS only) (Scored) 456
18.2.3 (L1) Ensure 'Enable Local Admin Password Management' is set to 'Enabled' (MS only) (Scored) 459
18.2.4 (L1) Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + special characters' (MS only) (Scored) 462

18.2.5 (L1) Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more' (MS only) (Scored) 465

18.2.6 (L1) Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer' (MS only) (Scored) 467

18.3 MS Security Guide 469

18.3.1 (L1) Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled' (MS only) (Scored) 469

18.3.2 (L1) Ensure 'Configure SMB v1 client' is set to 'Enabled: Bowser, MRxSmb20, NSI' (Scored) 472

18.3.3 (L1) Ensure 'Configure SMB v1 client driver' is set to 'Enabled: Disable driver (recommended)' (Scored) 474

18.3.4 (L1) Ensure 'Configure SMB v1 server' is set to 'Disabled' (Scored) 477

18.3.5 (L1) Ensure 'Enable Structured Exception Handling Overwrite Protection (SEHOP)' is set to 'Enabled' (Scored) 479

18.3.6 (L1) Ensure 'Extended Protection for LDAP Authentication (Domain Controllers only)' is set to 'Enabled: Enabled, always (recommended)' (DC Only) (Scored) 481

18.3.7 (L1) Ensure 'NetBT NodeType configuration' is set to 'Enabled: P-node (recommended)' (Scored) 484

18.3.8 (L1) Ensure 'WDigest Authentication' is set to 'Disabled' (Scored) 487

18.4 MSS (Legacy) 489

18.4.1 (L1) Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled' (Scored) 489

18.4.2 (L1) Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled' (Scored) 491

18.4.3 (L1) Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled' (Scored) 493

18.4.4 (L1) Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled' (Scored) 495

18.4.5 (L2) Ensure 'MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds' is set to 'Enabled: 300,000 or 5 minutes (recommended)' (Scored) 497

18.4.6 (L1) Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled' (Scored) 499

18.4.7 (L2) Ensure 'MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)' is set to 'Disabled' (Scored) 501

18.4.8 (L1) Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled' (Scored) 503

18.4.9 (L1) Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)' is set to 'Enabled: 5 or fewer seconds' (Scored) 506

18.4.10 (L2) Ensure 'MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3' (Scored) 508

18.4.11 (L2) Ensure 'MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3' (Scored) 510

18.4.12 (L1) Ensure 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' is set to 'Enabled: 90% or less' (Scored) 512

18.5 Network 515

18.5.1 Background Intelligent Transfer Service (BITS) 515

18.5.2 BranchCache 515

18.5.3 DirectAccess Client Experience Settings 515

18.5.4 DNS Client 516

18.5.4.1 (L1) Ensure 'Turn off multicast name resolution' is set to 'Enabled' (Scored) 516

18.5.5 Fonts 519

18.5.6 Hotspot Authentication 519

18.5.7 Lanman Server 519

18.5.8 Lanman Workstation 519

18.5.9 Link-Layer Topology Discovery 520

18.5.9.1 (L2) Ensure 'Turn on Mapper I/O (LLTDIO) driver' is set to 'Disabled' (Scored) 520

18.5.9.2 (L2) Ensure 'Turn on Responder (RSPNDR) driver' is set to 'Disabled' (Scored) 523

18.5.10 Microsoft Peer-to-Peer Networking Services 525
18.5.10.1 (L2) Ensure 'Turn off Microsoft Peer-to-Peer Networking Services' is set to 'Enabled' (Scored) 526
18.5.11 Network Connections 528
18.5.11.1 (L1) Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled' (Scored) 529
18.5.11.2 (L1) Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled' (Scored) 531
18.5.12 Network Connectivity Status Indicator 532
18.5.13 Network Isolation 532
18.5.14 Network Provider 533
18.5.14.1 (L1) Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares' (Scored) 533
18.5.15 Offline Files 536
18.5.16 QoS Packet Scheduler 536
18.5.17 SNMP 536
18.5.18 SSL Configuration Settings 536
18.5.19 TCPIP Settings 537
18.5.19.2.1 (L2) Disable IPv6 (Ensure TCPIP6 Parameter 'DisabledComponents' is set to '0xff (255)') (Scored) 538
18.5.20 Windows Connect Now 541
18.5.20.1 (L2) Ensure 'Configuration of wireless settings using Windows Connect Now' is set to 'Disabled' (Scored) 541
18.5.20.2 (L2) Ensure 'Prohibit access of the Windows Connect Now wizards' is set to 'Enabled' (Scored) 544
18.5.21 Windows Connection Manager 546
18.5.21.1 (L1) Ensure 'Minimize the number of simultaneous connections to the Internet or a Windows Domain' is set to 'Enabled: 1 = Minimize simultaneous connections' (Scored) 546
18.5.21.2 (L2) Ensure 'Prohibit connection to non-domain networks when connected to domain authenticated network' is set to 'Enabled' (MS only) (Scored) 548

18.6 Printers 550
18.7 Start Menu and Taskbar 551
18.7.1 Notifications 551
18.7.1.1 (L2) Ensure 'Turn off notifications network usage' is set to 'Enabled' (Scored) 551
18.8 System 553
18.8.1 Access-Denied Assistance 553
18.8.2 App-V 553
18.8.3 Audit Process Creation 554
18.8.3.1 (L1) Ensure 'Include command line in process creation events' is set to 'Disabled' (Scored) 554
18.8.4 Credentials Delegation 556
18.8.4.1 (L1) Ensure 'Encryption Oracle Remediation' is set to 'Enabled: Force Updated Clients' (Scored) 556
18.8.5 Device Guard 557
18.8.6 Device Health Attestation Service 558
18.8.7 Device Installation 558
18.8.8 Device Redirection 558
18.8.9 Disk NV Cache 558
18.8.10 Disk Quotas 559
18.8.11 Display 559
18.8.12 Distributed COM 559
18.8.13 Driver Installation 559
18.8.14 Early Launch Antimalware 560
18.8.14.1 (L1) Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good, unknown and bad but critical' (Scored) 560
18.8.15 Enhanced Storage Access 562
18.8.16 File Classification Infrastructure 562
18.8.17 File Share Shadow Copy Agent 562
18.8.18 File Share Shadow Copy Provider 563
18.8.19 Filesystem (formerly NTFS Filesystem) 563

18.8.20 Folder Redirection 563
18.8.21 Group Policy 564
18.8.21.1 (L1) Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE' (Scored) 564
18.8.21.2 (L1) Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE' (Scored) 567
18.8.21.3 (L1) Ensure 'Turn off background refresh of Group Policy' is set to 'Disabled' (Scored) 569
18.8.22 Internet Communication Management 571
18.8.22.1.1 (L1) Ensure 'Turn off downloading of print drivers over HTTP' is set to 'Enabled' (Scored) 571
18.8.22.1.2 (L2) Ensure 'Turn off handwriting personalization data sharing' is set to 'Enabled' (Scored) 573
18.8.22.1.3 (L2) Ensure 'Turn off handwriting recognition error reporting' is set to 'Enabled' (Scored) 575
18.8.22.1.4 (L2) Ensure 'Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com' is set to 'Enabled' (Scored) 577
18.8.22.1.5 (L1) Ensure 'Turn off Internet download for Web publishing and online ordering wizards' is set to 'Enabled' (Scored) 579
18.8.22.1.6 (L2) Ensure 'Turn off printing over HTTP' is set to 'Enabled' (Scored) 581
18.8.22.1.7 (L2) Ensure 'Turn off Registration if URL connection is referring to Microsoft.com' is set to 'Enabled' (Scored) 583
18.8.22.1.8 (L2) Ensure 'Turn off Search Companion content file updates' is set to 'Enabled' (Scored) 585
18.8.22.1.9 (L2) Ensure 'Turn off the "Order Prints" picture task' is set to 'Enabled' (Scored) 587
18.8.22.1.10 (L2) Ensure 'Turn off the "Publish to Web" task for files and folders' is set to 'Enabled' (Scored) 589
18.8.22.1.11 (L2) Ensure 'Turn off the Windows Messenger Customer Experience Improvement Program' is set to 'Enabled' (Scored) 591
18.8.22.1.12 (L2) Ensure 'Turn off Windows Customer Experience Improvement Program' is set to 'Enabled' (Scored) 593

18.8.22.1.13 (L2) Ensure 'Turn off Windows Error Reporting' is set to 'Enabled' (Scored) 595
18.8.23 iSCSI 597
18.8.24 KDC 597
18.8.25 Kerberos 597
18.8.26 Kernel DMA Protection 597
18.8.27 Locale Services 598
18.8.27.1 (L2) Ensure 'Disallow copying of user input methods to the system account for sign-in' is set to 'Enabled' (Scored) 598
18.8.28 Logon 600
18.8.28.1 (L1) Ensure 'Do not display network selection UI' is set to 'Enabled' (Scored) 600
18.8.28.2 (L1) Ensure 'Do not enumerate connected users on domain-joined computers' is set to 'Enabled' (Scored) 602
18.8.28.3 (L1) Ensure 'Enumerate local users on domain-joined computers' is set to 'Disabled' (MS only) (Scored) 604
18.8.28.4 (L1) Ensure 'Turn off app notifications on the lock screen' is set to 'Enabled' (Scored) 606
18.8.28.5 (L1) Ensure 'Turn off picture password sign-in' is set to 'Enabled' (Scored) 608
18.8.28.6 (L1) Ensure 'Turn on convenience PIN sign-in' is set to 'Disabled' (Scored) 610
18.8.29 Mitigation Options 612
18.8.30 Net Logon 612
18.8.31 OS Policies 612
18.8.32 Performance Control Panel 612
18.8.33 PIN Complexity 613
18.8.34 Power Management 614
18.8.34.6.1 (L1) Ensure 'Require a password when a computer wakes (on battery)' is set to 'Enabled' (Scored) 616
18.8.34.6.2 (L1) Ensure 'Require a password when a computer wakes (plugged in)' is set to 'Enabled' (Scored) 618
18.8.35 Recovery 619

18.8.36 Remote Assistance 620
18.8.36.1 (L1) Ensure 'Configure Offer Remote Assistance' is set to 'Disabled' (Scored) 620
18.8.36.2 (L1) Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled' (Scored) 622
18.8.37 Remote Procedure Call 624
18.8.37.1 (L1) Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled' (MS only) (Scored) 624
18.8.37.2 (L2) Ensure 'Restrict Unauthenticated RPC clients' is set to 'Enabled: Authenticated' (MS only) (Scored) 626
18.8.38 Removable Storage Access 628
18.8.39 Scripts 628
18.8.40 Server Manager 628
18.8.41 Service Control Manager Settings 629
18.8.42 Shutdown 629
18.8.43 Shutdown Options 629
18.8.44 Storage Health 629
18.8.45 Storage Sense 630
18.8.46 System Restore 630
18.8.47 Troubleshooting and Diagnostics 631
18.8.47.5.1 (L2) Ensure 'Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider' is set to 'Disabled' (Scored) 632
18.8.47.11.1 (L2) Ensure 'Enable/Disable PerfTrack' is set to 'Disabled' (Scored) 636
18.8.48 Trusted Platform Module Services 638
18.8.49 User Profiles 638
18.8.50 Windows File Protection 638
18.8.51 Windows HotStart 638
18.8.52 Windows Time Service 639
18.8.52.1.1 (L2) Ensure 'Enable Windows NTP Client' is set to 'Enabled' (Scored) 639

18.8.52.1.2 (L2) Ensure 'Enable Windows NTP Server' is set to 'Disabled' (MS only) (Scored) 641
18.9 Windows Components 643
18.9.1 Active Directory Federation Services 643
18.9.2 ActiveX Installer Service 643
18.9.3 Add features to Windows 8 / 8.1 / 10 (formerly Windows Anytime Upgrade) 643
18.9.4 App Package Deployment 644
18.9.5 App Privacy 644
18.9.6 App runtime 644
18.9.7 Application Compatibility 644
18.9.8 AutoPlay Policies 645
18.9.8.1 (L1) Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled' (Scored) 645
18.9.8.2 (L1) Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands' (Scored) 647
18.9.8.3 (L1) Ensure 'Turn off Autoplay' is set to 'Enabled: All drives' (Scored) 649
18.9.9 Backup 652
18.9.10 Biometrics 652
18.9.11 BitLocker Drive Encryption 652
18.9.12 Camera 652
18.9.13 Cloud Content 653
18.9.14 Connect 653
18.9.15 Credential User Interface 654
18.9.15.1 (L1) Ensure 'Do not display the password reveal button' is set to 'Enabled' (Scored) 654
18.9.15.2 (L1) Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled' (Scored) 656
18.9.16 Data Collection and Preview Builds 658
18.9.17 Delivery Optimization 658
18.9.18 Desktop Gadgets 658
18.9.19 Desktop Window Manager 658

18.9.20 Device and Driver Compatibility 659
18.9.21 Device Registration (formerly Workplace Join) 659
18.9.22 Digital Locker 659
18.9.23 Edge UI 659
18.9.24 EMET 660
18.9.24.1 (L1) Ensure 'EMET 5.52' or higher is installed (Scored) 661
18.9.24.2 (L1) Ensure 'Default Action and Mitigation Settings' is set to 'Enabled' (plus subsettings) (Scored) 663
18.9.24.3 (L1) Ensure 'Default Protections for Internet Explorer' is set to 'Enabled' (Scored) 665
18.9.24.4 (L1) Ensure 'Default Protections for Popular Software' is set to 'Enabled' (Scored) 667
18.9.24.5 (L1) Ensure 'Default Protections for Recommended Software' is set to 'Enabled' (Scored) 670
18.9.24.6 (L1) Ensure 'System ASLR' is set to 'Enabled: Application Opt-In' (Scored) 672
18.9.24.7 (L1) Ensure 'System DEP' is set to 'Enabled: Application Opt-Out' (Scored) 674
18.9.24.8 (L1) Ensure 'System SEHOP' is set to 'Enabled: Application Opt-Out' (Scored) 676
18.9.25 Event Forwarding 677
18.9.26 Event Log Service 678
18.9.26.1.1 (L1) Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Scored) 678
18.9.26.1.2 (L1) Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Scored) 680
18.9.26.2.1 (L1) Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Scored) 682
18.9.26.2.2 (L1) Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater' (Scored) 684
18.9.26.3.1 (L1) Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Scored) 686
18.9.26.3.2 (L1) Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Scored) 688

18.9.26.4.1 (L1) Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Scored) 690
18.9.26.4.2 (L1) Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Scored) 692
18.9.27 Event Logging 694
18.9.28 Event Viewer 694
18.9.29 Family Safety (formerly Parental Controls) 694
18.9.30 File Explorer (formerly Windows Explorer) 695
18.9.30.1 (L1) Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled' (Scored) 695
18.9.30.2 (L1) Ensure 'Turn off heap termination on corruption' is set to 'Disabled' (Scored) 698
18.9.30.3 (L1) Ensure 'Turn off shell protocol protected mode' is set to 'Disabled' (Scored) 700
18.9.31 File History 702
18.9.32 Find My Device 702
18.9.33 Game Explorer 702
18.9.34 Handwriting 702
18.9.35 HomeGroup 703
18.9.36 Import Video 703
18.9.37 Internet Explorer 703
18.9.38 Internet Information Services 703
18.9.39 Location and Sensors 704
18.9.39.1.1 (L2) Ensure 'Turn off Windows Location Provider' is set to 'Enabled' (Scored) 704
18.9.39.2 (L2) Ensure 'Turn off location' is set to 'Enabled' (Scored) 706
18.9.40 Maintenance Scheduler 707
18.9.41 Maps 707
18.9.42 MDM 708
18.9.43 Messaging 708
18.9.44 Microsoft account 708
18.9.45 Microsoft Edge 708

18.9.46 Microsoft FIDO Authentication 709
18.9.47 Microsoft Secondary Authentication Factor 709
18.9.48 Microsoft User Experience Virtualization 709
18.9.49 NetMeeting 709
18.9.50 Network Access Protection 710
18.9.51 Network Projector 710
18.9.52 OneDrive (formerly SkyDrive) 711
18.9.52.1 (L1) Ensure 'Prevent the usage of OneDrive for file storage' is set to 'Enabled' (Scored) 711
18.9.52.2 (L1) Ensure 'Prevent the usage of OneDrive for file storage on Windows 8.1' is set to 'Enabled' (Scored) 714
18.9.53 Online Assistance 716
18.9.54 OOBE 716
18.9.55 Password Synchronization 716
18.9.56 Portable Operating System 716
18.9.57 Presentation Settings 717
18.9.58 Push To Install 717
18.9.59 Remote Desktop Services (formerly Terminal Services) 718
18.9.59.2.2 (L1) Ensure 'Do not allow passwords to be saved' is set to 'Enabled' (Scored) 719
18.9.59.3.2.1 (L2) Ensure 'Restrict Remote Desktop Services users to a single Remote Desktop Services session' is set to 'Enabled' (Scored) 722
18.9.59.3.3.1 (L2) Ensure 'Do not allow COM port redirection' is set to 'Enabled' (Scored) 724
18.9.59.3.3.2 (L1) Ensure 'Do not allow drive redirection' is set to 'Enabled' (Scored) 726
18.9.59.3.3.3 (L2) Ensure 'Do not allow LPT port redirection' is set to 'Enabled' (Scored) 728
18.9.59.3.3.4 (L2) Ensure 'Do not allow supported Plug and Play device redirection' is set to 'Enabled' (Scored) 730
18.9.59.3.9.1 (L1) Ensure 'Always prompt for password upon connection' is set to 'Enabled' (Scored) 733

18.9.59.3.9.2 (L1) Ensure 'Require secure RPC communication' is set to 'Enabled' (Scored) 736
18.9.59.3.9.3 (L1) Ensure 'Require use of specific security layer for remote (RDP) connections' is set to 'Enabled: SSL' (Scored) 738
18.9.59.3.9.4 (L1) Ensure 'Require user authentication for remote connections by using Network Level Authentication' is set to 'Enabled' (Scored) 741
18.9.59.3.9.5 (L1) Ensure 'Set client connection encryption level' is set to 'Enabled: High Level' (Scored) 743
18.9.59.3.10.1 (L2) Ensure 'Set time limit for active but idle Remote Desktop Services sessions' is set to 'Enabled: 15 minutes or less' (Scored) 745
18.9.59.3.10.2 (L2) Ensure 'Set time limit for disconnected sessions' is set to 'Enabled: 1 minute' (Scored) 748
18.9.59.3.11.1 (L1) Ensure 'Do not delete temp folders upon exit' is set to 'Disabled' (Scored) 750
18.9.59.3.11.2 (L1) Ensure 'Do not use temporary folders per session' is set to 'Disabled' (Scored) 752
18.9.60 RSS Feeds 754
18.9.60.1 (L1) Ensure 'Prevent downloading of enclosures' is set to 'Enabled' (Scored) 754
18.9.61 Search 756
18.9.61.2 (L1) Ensure 'Allow indexing of encrypted files' is set to 'Disabled' (Scored) 756
18.9.62 Security Center 758
18.9.63 Server for NIS 758
18.9.64 Shutdown Options 758
18.9.65 Smart Card 758
18.9.66 Software Protection Platform 759
18.9.66.1 (L2) Ensure 'Turn off KMS Client Online AVS Validation' is set to 'Enabled' (Scored) 759
18.9.67 Sound Recorder 760
18.9.68 Speech 761
18.9.69 Store 761
18.9.70 Sync your settings 761

18.9.71 Tablet PC 761
18.9.72 Task Scheduler 762
18.9.73 Text Input 762
18.9.74 Windows Calendar 762
18.9.75 Windows Color System 762
18.9.76 Windows Customer Experience Improvement Program 762
18.9.77 Windows Defender Antivirus (formerly Windows Defender) 763
18.9.77.3.1 (L1) Ensure 'Configure local setting override for reporting to Microsoft MAPS' is set to 'Disabled' (Scored) 764
18.9.77.3.2 (L2) Ensure 'Join Microsoft MAPS' is set to 'Disabled' (Scored) 766
18.9.77.7.1 (L1) Ensure 'Turn on behavior monitoring' is set to 'Enabled' (Scored) 769
18.9.77.9.1 (L2) Ensure 'Configure Watson events' is set to 'Disabled' (Scored) 772
18.9.77.10.1 (L1) Ensure 'Scan removable drives' is set to 'Enabled' (Scored) ... 774
18.9.77.10.2 (L1) Ensure 'Turn on e-mail scanning' is set to 'Enabled' (Scored) 776
18.9.77.14 (L1) Ensure 'Turn off Windows Defender AntiVirus' is set to 'Disabled' (Scored) 779
18.9.78 Windows Defender Application Guard 781
18.9.79 Windows Defender Exploit Guard 781
18.9.80 Windows Defender SmartScreen 782
18.9.80.1.1 (L1) Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled: Warn and prevent bypass' (Scored) 782
18.9.81 Windows Error Reporting 785
18.9.81.2.1 (L1) Ensure 'Configure Default consent' is set to 'Enabled: Always ask before sending data' (Scored) 786
18.9.82 Windows Game Recording and Broadcasting 788
18.9.83 Windows Hello for Business (formerly Microsoft Passport for Work) 788
18.9.84 Windows Ink Workspace 788
18.9.85 Windows Installer 789
18.9.85.1 (L1) Ensure 'Allow user control over installs' is set to 'Disabled' (Scored) 789

18.9.85.2 (L1) Ensure 'Always install with elevated privileges' is set to 'Disabled' (Scored) 792
18.9.85.3 (L2) Ensure 'Prevent Internet Explorer security prompt for Windows Installer scripts' is set to 'Disabled' (Scored) 794
18.9.86 Windows Logon Options 795
18.9.87 Windows Mail 795
18.9.88 Windows Media Center 796
18.9.89 Windows Media Digital Rights Management 796
18.9.90 Windows Media Player 796
18.9.91 Windows Meeting Space 796
18.9.92 Windows Messenger 797
18.9.93 Windows Mobility Center 797
18.9.94 Windows Movie Maker 797
18.9.95 Windows PowerShell 798
18.9.95.1 (L1) Ensure 'Turn on PowerShell Script Block Logging' is set to 'Disabled' (Scored) 798
18.9.95.2 (L1) Ensure 'Turn on PowerShell Transcription' is set to 'Disabled' (Scored) 800
18.9.96 Windows Reliability Analysis 801
18.9.97 Windows Remote Management (WinRM) 802
18.9.97.1.1 (L1) Ensure 'Allow Basic authentication' is set to 'Disabled' (Scored) 802
18.9.97.1.2 (L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled' (Scored) 805
18.9.97.1.3 (L1) Ensure 'Disallow Digest authentication' is set to 'Enabled' (Scored) 807
18.9.97.2.1 (L1) Ensure 'Allow Basic authentication' is set to 'Disabled' (Scored) 809
18.9.97.2.2 (L2) Ensure 'Allow remote server management through WinRM' is set to 'Disabled' (Scored) 811
18.9.97.2.3 (L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled' (Scored) 813

18.9.97.2.4 (L1) Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled' (Scored) 815
18.9.98 Windows Remote Shell 817
18.9.98.1 (L2) Ensure 'Allow Remote Shell Access' is set to 'Disabled' (Scored) 817
18.9.99 Windows Security (formerly Windows Defender Security Center) 819
18.9.100 Windows SideShow 820
18.9.101 Windows System Resource Manager 820
18.9.102 Windows Update 821
18.9.102.1 (L1) Ensure 'Configure Automatic Updates' is set to 'Enabled' (Scored) 821
18.9.102.2 (L1) Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day' (Scored) 824
18.9.102.3 (L1) Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled' (Scored) 826
19 Administrative Templates (User) 829
19.1 Control Panel 829
19.1.1 Add or Remove Programs 829
19.1.2 Display 829
19.1.3 Personalization (formerly Desktop Themes) 830
19.1.3.1 (L1) Ensure 'Enable screen saver' is set to 'Enabled' (Scored) 830
19.1.3.2 (L1) Ensure 'Force specific screen saver: Screen saver executable name' is set to 'Enabled: scrnsave.scr' (Scored) 832
19.1.3.3 (L1) Ensure 'Password protect the screen saver' is set to 'Enabled' (Scored) 834
19.1.3.4 (L1) Ensure 'Screen saver timeout' is set to 'Enabled: 900 seconds or fewer, but not 0' (Scored) 836
19.2 Desktop 838
19.3 Network 838
19.4 Shared Folders 838
19.5 Start Menu and Taskbar 839
19.5.1 Notifications 839

19.5.1.1 (L1) Ensure 'Turn off toast notifications on the lock screen' is set to 'Enabled' (Scored) 839
19.6 System 841
19.6.1 Ctrl+Alt+Del Options 841
19.6.2 Display 841
19.6.3 Driver Installation 841
19.6.4 Folder Redirection 841
19.6.5 Group Policy 842
19.6.6 Internet Communication Management 843
19.6.6.1.1 (L2) Ensure 'Turn off Help Experience Improvement Program' is set to 'Enabled' (Scored) 843
19.7 Windows Components 845
19.7.1 Add features to Windows 8 / 8.1 / 10 (formerly Windows Anytime Upgrade) 845
19.7.2 App runtime 845
19.7.3 Application Compatibility 845
19.7.4 Attachment Manager 846
19.7.4.1 (L1) Ensure 'Do not preserve zone information in file attachments' is set to 'Disabled' (Scored) 846
19.7.4.2 (L1) Ensure 'Notify antivirus programs when opening attachments' is set to 'Enabled' (Scored) 848
19.7.5 AutoPlay Policies 850
19.7.6 Backup 850
19.7.7 Cloud Content 850
19.7.8 Credential User Interface 850
19.7.9 Data Collection and Preview Builds 851
19.7.10 Desktop Gadgets 851
19.7.11 Desktop Window Manager 851
19.7.12 Digital Locker 851
19.7.13 Edge UI 852
19.7.14 File Explorer (formerly Windows Explorer) 852
19.7.15 File Revocation 852

19.7.16 IME 852
19.7.17 Import Video 853
19.7.18 Instant Search 853
19.7.19 Internet Explorer 853
19.7.20 Location and Sensors 853
19.7.21 Microsoft Edge 853
19.7.22 Microsoft Management Console 854
19.7.23 Microsoft User Experience Virtualization 854
19.7.24 NetMeeting 854
19.7.25 Network Projector 854
19.7.26 Network Sharing 855
19.7.26.1 (L1) Ensure 'Prevent users from sharing files within their profile.' is set to 'Enabled' (Scored) 855
19.7.27 OOBE 857
19.7.28 Presentation Settings 857
19.7.29 Remote Desktop Services (formerly Terminal Services) 857
19.7.30 RSS Feeds 857
19.7.31 Search 858
19.7.32 Sound Recorder 858
19.7.33 Store 858
19.7.34 Tablet PC 858
19.7.35 Task Scheduler 859
19.7.36 Windows Calendar 859
19.7.37 Windows Color System 859
19.7.38 Windows Defender SmartScreen 859
19.7.39 Windows Error Reporting 860
19.7.40 Windows Hello for Business (formerly Microsoft Passport for Work) 860
19.7.41 Windows Installer 861
19.7.41.1 (L1) Ensure 'Always install with elevated privileges' is set to 'Disabled' (Scored) 861
19.7.42 Windows Logon Options 863

19.7.43 Windows Mail 863
19.7.44 Windows Media Center 863
19.7.45 Windows Media Player 864
19.7.45.2.1 (L2) Ensure 'Prevent Codec Download' is set to 'Enabled' (Scored) . 865
Appendix: Summary Table 867
Appendix: Change History 896

Overview

This document provides prescriptive guidance for establishing a secure configuration posture for Microsoft Windows Server 2012. This guide was tested against Microsoft Windows Server 2012 Datacenter. To obtain the latest version of this 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 benchmark was created using a consensus review process comprised of subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

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

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
Monospace font	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

Scoring Information

A scoring status indicates whether compliance with the given recommendation impacts the assessed target's benchmark score. The following scoring statuses are used in this benchmark:

Scored

Failure to comply with "Scored" recommendations will decrease the final benchmark score. Compliance with "Scored" recommendations will increase the final benchmark score.

Not Scored

Failure to comply with "Not Scored" recommendations will not decrease the final benchmark score. Compliance with "Not Scored" recommendations will not increase the final benchmark score.

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

Acknowledgements

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

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

Contributor
Jennifer Jarose
Jason Braun
Jordan Rakoske GSEC, GCWN
Phil White CISSP, PMP
Matt Woods

Editor
Haemish Edgerton MCSE:Security, MCITP:EA
Hardeep Mehrotara CISSP, CISA, CICP
Kevin Zhang CISSP, CISA, CRISC, CSSLP

Recommendations

1 Account Policies

This section contains recommendations for account policies.

1.1 Password Policy

This section contains recommendations for password policy.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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 Windows Vista is 0 passwords, but the default setting in a domain is 24 passwords. To maintain the effectiveness of this policy setting, use the Minimum password age setting to prevent users from repeatedly changing their password.

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

Rationale:

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

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

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
```

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.

Default Value:

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

References:

1. CCE-37166-6

CIS Controls:

Version 6

16.5 Ensure Workstation Screen Locks Are Configured
Configure screen locks on systems to limit access to unattended workstations.

Version 7

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.

16.5 Encrypt Transmittal of Username and Authentication Credentials
Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.

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

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 `60 or fewer days, but not 0`.

Rationale:

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

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
```

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.

Default Value:

42 days.

References:

1. CCE-37167-4

CIS Controls:

Version 6

16.5 Ensure Workstation Screen Locks Are Configured
Configure screen locks on systems to limit access to unattended workstations.

Version 7

16.10 Ensure All Accounts Have An Expiration Date
Ensure that all accounts have an expiration date that is monitored and enforced.

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.

16.5 Encrypt Transmittal of Username and Authentication Credentials
Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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)`.

Rationale:

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

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
```

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.

Default Value:

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

References:

1. CCE-37073-4

CIS Controls:

Version 6

16.5 Ensure Workstation Screen Locks Are Configured
Configure screen locks on systems to limit access to unattended workstations.

Version 7

16.10 Ensure All Accounts Have An Expiration Date
Ensure that all accounts have an expiration date that is monitored and enforced.

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.

16.5 Encrypt Transmittal of Username and Authentication Credentials
Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.

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

Profile Applicability:

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

Description:

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

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.

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
```

Impact:

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

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

Default Value:

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

References:

1. CCE-36534-6

CIS Controls:

Version 6

5.7 User Accounts Shall Use Long Passwords

Where multi-factor authentication is not supported, user accounts shall be required to use long passwords on the system (longer than 14 characters).

16.12 Use Long Passwords For All User Accounts

Where multi-factor authentication is not supported, user accounts shall be required to use long passwords on the system (longer than 14 characters).

16.5 Ensure Workstation Screen Locks Are Configured

Configure screen locks on systems to limit access to unattended workstations.

Version 7

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.

16.5 Encrypt Transmittal of Username and Authentication Credentials

Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.

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

Profile Applicability:

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

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

Rationale:

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

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
```

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.)

Default Value:

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

References:

1. CCE-37063-5

CIS Controls:

Version 6

16.5 Ensure Workstation Screen Locks Are Configured
Configure screen locks on systems to limit access to unattended workstations.

Version 7

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.

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.

16.5 Encrypt Transmittal of Username and Authentication Credentials
Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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`.

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.

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
```

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.

Default Value:

Disabled.

References:

1. CCE-36286-3

CIS Controls:

Version 6

16.14 Encrypt/Hash All Authentication Files And Monitor Their Access
Verify that all authentication files are encrypted or hashed and that these files cannot be accessed without root or administrator privileges. Audit all access to password files in the system.

16.5 Ensure Workstation Screen Locks Are Configured
Configure screen locks on systems to limit access to unattended workstations.

Version 7

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.

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

16.5 Encrypt Transmittal of Username and Authentication Credentials
Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.

1.2 Account Lockout Policy

This section contains recommendations for account lockout policy.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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)`.

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.

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
```

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.

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. CCE-37034-6

CIS Controls:

Version 6

16 Account Monitoring and Control
Account Monitoring and Control

16.7 Configure Account Lockouts
Use and configure account lockouts such that after a set number of failed login attempts the account is locked for a standard period of time.

Version 7

16.11 Lock Workstation Sessions After Inactivity
Automatically lock workstation sessions after a standard period of inactivity.

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.

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

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: `10 or fewer invalid logon attempt(s), but not 0`.

Rationale:

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

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 invalid login attempt(s), but not 0`:

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

Impact:

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

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

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

Default Value:

0 failed logon attempts.

References:

1. CCE-36008-1

CIS Controls:

Version 6

16 Account Monitoring and Control
Account Monitoring and Control

16.7 Configure Account Lockouts
Use and configure account lockouts such that after a set number of failed login attempts the account is locked for a standard period of time.

Version 7

16.11 Lock Workstation Sessions After Inactivity
Automatically lock workstation sessions after a standard period of inactivity.

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.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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).`

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.

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
```

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.

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. CCE-36883-7

CIS Controls:

Version 6

16 Account Monitoring and Control
Account Monitoring and Control

16.7 Configure Account Lockouts
Use and configure account lockouts such that after a set number of failed login attempts the account is locked for a standard period of time.

Version 7

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.

16.5 Encrypt Transmittal of Username and Authentication Credentials
Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.

2 Local Policies

This section contains recommendations for local policies.

2.1 Audit Policy

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

2.2 User Rights Assignment

This section contains recommendations for user rights assignments.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

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
```

Impact:

None - this is the default behavior.

Default Value:

No one.

References:

1. CCE-37056-9

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

4.8 Log and Alert on Changes to Administrative Group Membership

Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.

2.2.2 (L1) Ensure 'Access this computer from the network' is set to 'Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS' (DC only) (Scored)

Profile Applicability:

- Level 1 - 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.

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\Access this computer from the network
```

Impact:

If you remove the **Access this computer from the network** user right on Domain Controllers for all users, no one will be able to log on to the domain or use network resources. If you remove this user right on Member Servers, users will not be able to connect to those servers through the network. Successful negotiation of IPsec connections requires that the initiating machine has this right, therefore if using IPsec, it is recommended that it 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.

Default Value:

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

References:

1. CCE-35818-4

CIS Controls:

Version 6

9 Limitation and Control of Network Ports, Protocols, and Services
Limitation and Control of Network Ports, Protocols, and Services

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

2.2.3 (L1) Ensure 'Access this computer from the network' is set to 'Administrators, Authenticated Users' (MS only) (Scored)

Profile Applicability:

- Level 1 - 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.

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\Access this computer from the network
```

Impact:

If you remove the **Access this computer from the network** user right on Domain Controllers for all users, no one will be able to log on to the domain or use network resources. If you remove this user right on Member Servers, users will not be able to connect to those servers through the network. Successful negotiation of IPsec connections requires that the initiating machine has this right, therefore if using IPsec, it is recommended that it 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.

Default Value:

Administrators, Backup Operators, Users, Everyone.

References:

1. CCE-35818-4

CIS Controls:

Version 6

9 Limitation and Control of Network Ports, Protocols, and Services
Limitation and Control of Network Ports, Protocols, and Services

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

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
```

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.

Default Value:

No one.

References:

1. CCE-36876-1

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

4.8 Log and Alert on Changes to Administrative Group Membership

Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.

2.2.5 (L1) Ensure 'Add workstations to domain' is set to 'Administrators' (DC only) (Scored)

Profile Applicability:

- Level 1 - 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.

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
```

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.

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.)

References:

1. CCE-36282-2

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

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.

4.5 Use Multifactor Authentication For All Administrative Access

Use multi-factor authentication and encrypted channels for all administrative account access.

4.8 Log and Alert on Changes to Administrative Group Membership

Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.

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

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.

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
```

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.

Default Value:

Administrators, LOCAL SERVICE, NETWORK SERVICE.

References:

1. CCE-37071-8

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

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.

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.

4.8 Log and Alert on Changes to Administrative Group Membership

Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.

2.2.7 (L1) Ensure 'Allow log on locally' is set to 'Administrators' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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`.

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.

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.

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
```

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.

Default Value:

On Member Servers: Administrators, Backup Operators, Users.

On Domain Controllers: Account Operators, Administrators, Backup Operators, Print Operators.

References:

1. CCE-37659-0

CIS Controls:

Version 6

16 Account Monitoring and Control
Account Monitoring and Control

Version 7

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.

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.

4.5 Use Multifactor Authentication For All Administrative Access
Use multi-factor authentication and encrypted channels for all administrative account access.

2.2.8 (L1) Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators' (DC only) (Scored)

Profile Applicability:

- Level 1 - 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.

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
```

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.

Default Value:

Administrators.

References:

1. CCE-37072-6

CIS Controls:

Version 6

16 Account Monitoring and Control
Account Monitoring and Control

Version 7

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.

4.6 Use of Dedicated Machines For All Administrative Tasks
Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.

4.8 Log and Alert on Changes to Administrative Group Membership
Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

2.2.9 (L1) Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators, Remote Desktop Users' (MS only) (Scored)

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.

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
```

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.

Default Value:

Administrators, Remote Desktop Users.

References:

1. CCE-37072-6

CIS Controls:

Version 6

16 Account Monitoring and Control
Account Monitoring and Control

Version 7

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.

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.

4.5 Use Multifactor Authentication For All Administrative Access
Use multi-factor authentication and encrypted channels for all administrative account access.

4.6 Use of Dedicated Machines For All Administrative Tasks
Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.

4.8 Log and Alert on Changes to Administrative Group Membership
Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

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
```

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.

Default Value:

On Member Servers: Administrators, Backup Operators.

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

References:

1. CCE-35912-5

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

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.

4.6 Use of Dedicated Machines For All Administrative Tasks

Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.

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

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.

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
```

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.

Default Value:

On Member Servers: Administrators, LOCAL SERVICE.

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

References:

1. CCE-37452-0

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

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.

4.6 Use of Dedicated Machines For All Administrative Tasks
Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.

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

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.

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
```

Impact:

None - this is the default behavior.

Default Value:

Administrators, LOCAL SERVICE.

References:

1. CCE-37700-2

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

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.

4.6 Use of Dedicated Machines For All Administrative Tasks

Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

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
```

Impact:

None - this is the default behavior.

Default Value:

Administrators.

References:

1. CCE-35821-8

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

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.

4.6 Use of Dedicated Machines For All Administrative Tasks

Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

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
```

Impact:

None - this is the default behavior.

Default Value:

No one.

References:

1. CCE-36861-3

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

4.8 Log and Alert on Changes to Administrative Group Membership

Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

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
```

Impact:

None - this is the default behavior.

Default Value:

Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE.

References:

1. CCE-37453-8

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

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.

4.6 Use of Dedicated Machines For All Administrative Tasks

Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

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
```

Impact:

None - this is the default behavior.

Default Value:

No one.

References:

1. CCE-36532-0

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

4.8 Log and Alert on Changes to Administrative Group Membership

Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.

2.2.17 (L1) Ensure 'Create symbolic links' is set to 'Administrators' (DC only) (Scored)

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.

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
```

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.

Default Value:

Administrators.

References:

1. CCE-35823-4

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

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.

4.6 Use of Dedicated Machines For All Administrative Tasks

Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.

2.2.18 (L1) Ensure 'Create symbolic links' is set to 'Administrators, NT VIRTUAL MACHINE\Virtual Machines' (MS only) (Scored)

Profile Applicability:

- Level 1 - 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.

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
```

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.

Default Value:

Administrators.

References:

1. CCE-35823-4

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

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.

4.6 Use of Dedicated Machines For All Administrative Tasks

Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.

2.2.19 (L1) Ensure 'Debug programs' is set to 'Administrators' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

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
```

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.

Default Value:

Administrators.

References:

1. CCE-37075-9

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

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.

4.6 Use of Dedicated Machines For All Administrative Tasks

Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.

2.2.20 (L1) Ensure 'Deny access to this computer from the network' to include 'Guests' (DC only) (Scored)

Profile Applicability:

- Level 1 - 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.

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
```

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.

Default Value:

Guest.

References:

1. CCE-37954-5

CIS Controls:

Version 6

16 Account Monitoring and Control
Account Monitoring and Control

Version 7

16.8 Disable Any Unassociated Accounts
Disable any account that cannot be associated with a business process or business owner.

2.2.21 (L1) Ensure 'Deny access to this computer from the network' to include 'Guests, Local account and member of Administrators group' (MS only) (Scored)

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.

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
```

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.

Default Value:

No one.

References:

1. CCE-37954-5

CIS Controls:

Version 6

16 Account Monitoring and Control
Account Monitoring and Control

Version 7

16.8 Disable Any Unassociated Accounts
Disable any account that cannot be associated with a business process or business owner.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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 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.

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
```

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.

Default Value:

No one.

References:

1. CCE-36923-1

CIS Controls:

Version 6

16 Account Monitoring and Control
Account Monitoring and Control

Version 7

16.8 Disable Any Unassociated Accounts
Disable any account that cannot be associated with a business process or business owner.

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

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.

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
```

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.

Default Value:

No one.

References:

1. CCE-36877-9

CIS Controls:

Version 6

16 Account Monitoring and Control
Account Monitoring and Control

Version 7

16.8 Disable Any Unassociated Accounts
Disable any account that cannot be associated with a business process or business owner.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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`.

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.

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
```

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.

Default Value:

No one.

References:

1. CCE-37146-8

CIS Controls:

Version 6

16 Account Monitoring and Control
Account Monitoring and Control

Version 7

16.8 Disable Any Unassociated Accounts
Disable any account that cannot be associated with a business process or business owner.

2.2.25 (L1) Ensure 'Deny log on through Remote Desktop Services' to include 'Guests' (DC only) (Scored)

Profile Applicability:

- Level 1 - 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.

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
```

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.

Default Value:

No one.

References:

1. CCE-36867-0

CIS Controls:

Version 6

16 Account Monitoring and Control
Account Monitoring and Control

Version 7

16.8 Disable Any Unassociated Accounts
Disable any account that cannot be associated with a business process or business owner.

2.2.26 (L1) Ensure 'Deny log on through Remote Desktop Services' is set to 'Guests, Local account' (MS only) (Scored)

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.

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
```

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.

Default Value:

No one.

References:

1. CCE-36867-0

CIS Controls:

Version 6

16 Account Monitoring and Control
Account Monitoring and Control

Version 7

16.8 Disable Any Unassociated Accounts
Disable any account that cannot be associated with a business process or business owner.

2.2.27 (L1) Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'Administrators' (DC only) (Scored)

Profile Applicability:

- Level 1 - 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.

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
```

Impact:

None - this is the default behavior.

Default Value:

Administrators.

References:

1. CCE-36860-5

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

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.

4.6 Use of Dedicated Machines For All Administrative Tasks

Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.

2.2.28 (L1) Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'No One' (MS only) (Scored)

Profile Applicability:

- Level 1 - 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.

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
```

Impact:

None - this is the default behavior.

Default Value:

No one.

References:

1. CCE-36860-5

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

4.8 Log and Alert on Changes to Administrative Group Membership

Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.

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

Profile Applicability:

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

Description:

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

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

Rationale:

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

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
```

Impact:

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

Default Value:

On Member Servers: Administrators.

On Domain Controllers: Administrators, Server Operators.

References:

1. CCE-37877-8

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

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.

4.6 Use of Dedicated Machines For All Administrative Tasks

Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

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
```

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.

Default Value:

LOCAL SERVICE, NETWORK SERVICE.

References:

1. CCE-37639-2

CIS Controls:

Version 6

16 Account Monitoring and Control
Account Monitoring and Control

Version 7

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.

2.2.31 (L1) Ensure 'Impersonate a client after authentication' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (DC only) (Scored)

Profile Applicability:

- Level 1 - 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.

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
```

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`.

Default Value:

Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE.

References:

1. CCE-37106-2

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

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.

4.6 Use of Dedicated Machines For All Administrative Tasks

Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.

2.2.32 (L1) 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) (Scored)

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.

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
```

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`.

Default Value:

Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE.

References:

1. CCE-37106-2

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

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.

4.6 Use of Dedicated Machines For All Administrative Tasks

Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.

2.2.33 (L1) Ensure 'Increase scheduling priority' is set to 'Administrators' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

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
```

Impact:

None - this is the default behavior.

Default Value:

On Windows Server 2016 or older: Administrators.

On Windows Server 2019 or newer: Administrators, Window Manager\Window Manager Group.

References:

1. CCE-38326-5

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

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.

4.6 Use of Dedicated Machines For All Administrative Tasks

Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

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
```

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.

Default Value:

On Member Servers: Administrators.

On Domain Controllers: Administrators, Print Operators.

References:

1. CCE-36318-4

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

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.

4.6 Use of Dedicated Machines For All Administrative Tasks
Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

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
```

Impact:

None - this is the default behavior.

Default Value:

No one.

References:

1. CCE-36495-0

CIS Controls:

Version 6

16 Account Monitoring and Control
Account Monitoring and Control

Version 7

4.8 Log and Alert on Changes to Administrative Group Membership
Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.

2.2.36 (L2) Ensure 'Log on as a batch job' is set to 'Administrators' (DC Only) (Scored)

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.

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
```

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.

Default Value:

Administrators, Backup Operators.

References:

1. CCE-38080-8

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

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.

2.2.37 (L1) Ensure 'Manage auditing and security log' is set to 'Administrators' and (when Exchange is running in the environment) 'Exchange Servers' (DC only) (Scored)

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.

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` and (when Exchange is running in the environment) `Exchange Servers`.

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.

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
```

Impact:

None - this is the default behavior.

Default Value:

Administrators.

References:

1. CCE-35906-7

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

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.

4.6 Use of Dedicated Machines For All Administrative Tasks
Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.

6.5 Central Log Management
Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.

2.2.38 (L1) Ensure 'Manage auditing and security log' is set to 'Administrators' (MS only) (Scored)

Profile Applicability:

- Level 1 - 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.

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
```

Impact:

None - this is the default behavior.

Default Value:

Administrators.

References:

1. CCE-35906-7

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

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.

4.6 Use of Dedicated Machines For All Administrative Tasks

Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.

6.5 Central Log Management

Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.

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

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.

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
```

Impact:

None - this is the default behavior.

Default Value:

No one.

References:

1. CCE-36054-5

CIS Controls:

Version 6

16 Account Monitoring and Control
Account Monitoring and Control

Version 7

4.8 Log and Alert on Changes to Administrative Group Membership
Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

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
```

Impact:

None - this is the default behavior.

Default Value:

Administrators.

References:

1. CCE-38113-7

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

4.6 Use of Dedicated Machines For All Administrative Tasks

Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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`.

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.

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
```

Impact:

None - this is the default behavior.

Default Value:

Administrators.

References:

1. CCE-36143-6

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

4.6 Use of Dedicated Machines For All Administrative Tasks

Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

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
```

Impact:

None - this is the default behavior.

Default Value:

Administrators.

References:

1. CCE-37131-0

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

4.6 Use of Dedicated Machines For All Administrative Tasks

Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.

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

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.

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
```

Impact:

None - this is the default behavior.

Default Value:

Windows Server 2008 (non-R2): Administrators.

Windows Server 2008 R2 and newer: Administrators, NT SERVICE\WdiServiceHost.

References:

1. CCE-36052-9

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

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.

4.6 Use of Dedicated Machines For All Administrative Tasks

Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.

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

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.)

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
```

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.

Default Value:

LOCAL SERVICE, NETWORK SERVICE.

References:

1. CCE-37430-6

CIS Controls:

Version 6

16 Account Monitoring and Control
Account Monitoring and Control

Version 7

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.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

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
```

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.

Default Value:

On Member Servers: Administrators, Backup Operators.

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

References:

1. CCE-37613-7

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

4.6 Use of Dedicated Machines For All Administrative Tasks
Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.

2.2.46 (L1) Ensure 'Shut down the system' is set to 'Administrators' (Scored)

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.

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
```

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.

Default Value:

On Member Servers: Administrators, Backup Operators.

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

References:

1. CCE-38328-1

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

4.6 Use of Dedicated Machines For All Administrative Tasks

Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.

2.2.47 (L1) Ensure 'Synchronize directory service data' is set to 'No One' (DC only) (Scored)

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.

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
```

Impact:

None - this is the default behavior.

Default Value:

No one.

References:

1. CCE-36099-0

CIS Controls:

Version 6

16 Account Monitoring and Control
Account Monitoring and Control

Version 7

4.8 Log and Alert on Changes to Administrative Group Membership
Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

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
```

Impact:

None - this is the default behavior.

Default Value:

Administrators.

References:

1. CCE-38325-7

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

4.6 Use of Dedicated Machines For All Administrative Tasks

Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.

2.3 Security Options

This section contains recommendations for security options.

2.3.1 Accounts

This section contains recommendations related to default accounts.

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

Profile Applicability:

- Level 1 - Member Server

Description:

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

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

Rationale:

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

Audit:

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

Remediation:

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

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

Impact:

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

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

Default Value:

Disabled.

References:

1. CCE-37953-7

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

16.8 Disable Any Unassociated Accounts

Disable any account that cannot be associated with a business process or business owner.

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

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

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

Remediation:

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

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

Impact:

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

Default Value:

Users are able to use Microsoft accounts with Windows.

References:

1. CCE-36147-7

CIS Controls:

Version 6

16 Account Monitoring and Control
Account Monitoring and Control

Version 7

16.8 Disable Any Unassociated Accounts
Disable any account that cannot be associated with a business process or business owner.

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

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.

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
```

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.

Default Value:

Disabled.

References:

1. CCE-37432-2

CIS Controls:

Version 6

16.1 Perform Regular Account Reviews
Review all system accounts and disable any account that cannot be associated with a business process and owner.

Version 7

16.8 Disable Any Unassociated Accounts
Disable any account that cannot be associated with a business process or business owner.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa:LimitBlankPasswordUse
```

Remediation:

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

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

Impact:

None - this is the default behavior.

Default Value:

Enabled.

References:

1. CCE-37615-2

CIS Controls:

Version 6

16 Account Monitoring and Control
Account Monitoring and Control

Version 7

4.4 Use Unique Passwords
Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

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
```

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.)

Default Value:

Administrator.

References:

1. CCE-38233-3

CIS Controls:

Version 6

16 Account Monitoring and Control
Account Monitoring and Control

Version 7

16.8 Disable Any Unassociated Accounts
Disable any account that cannot be associated with a business process or business owner.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

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
```

Impact:

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

Default Value:

Guest.

References:

1. CCE-38027-9

CIS Controls:

Version 6

16 Account Monitoring and Control
Account Monitoring and Control

Version 7

16.8 Disable Any Unassociated Accounts
Disable any account that cannot be associated with a business process or business owner.

2.3.2 Audit

This section contains recommendations related to auditing controls.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa:SCENoApplyLegacyAudit
Policy
```

Remediation:

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

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

Impact:

None - this is the default behavior.

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. CCE-37850-5

CIS Controls:

Version 6

6.2 Ensure Audit Log Settings Support Appropriate Log Entry Formatting

Validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction. Systems should record logs in a standardized format such as syslog entries or those outlined by the Common Event Expression initiative. If systems cannot generate logs in a standardized format, log normalization tools can be deployed to convert logs into such a format.

Version 7

6.2 Activate audit logging

Ensure that local logging has been enabled on all systems and networking devices.

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

6.4 Ensure adequate storage for logs

Ensure that all systems that store logs have adequate storage space for the logs generated.

6.5 Central Log Management

Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.

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

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa:CrashOnAuditFail
```

Remediation:

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

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

Impact:

None - this is the default behavior.

Default Value:

Disabled.

References:

1. CCE-35907-5

CIS Controls:

Version 6

6 Maintenance, Monitoring, and Analysis of Audit Logs
Maintenance, Monitoring, and Analysis of Audit Logs

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

6.3 Enable Detailed Logging
Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

6.4 Ensure adequate storage for logs
Ensure that all systems that store logs have adequate storage space for the logs generated.

6.5 Central Log Management
Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.

2.3.3 DCOM

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

2.3.4 Devices

This section contains recommendations related to managing devices.

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

Profile Applicability:

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

Description:

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

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

Rationale:

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

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

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

Remediation:

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

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

Impact:

None - this is the default behavior.

Default Value:

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

References:

1. CCE-37701-0

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

4.6 Use of Dedicated Machines For All Administrative Tasks

Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.

8.4 Configure Anti-Malware Scanning of Removable Devices

Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.

13.7 Manage USB Devices

If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained.

2.3.4.2 (L1) Ensure 'Devices: Prevent users from installing printer drivers' is set to 'Enabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Providers\LanMan
Print Services\Servers:AddPrinterDrivers
```

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Devices: Prevent users from installing printer
drivers
```

Impact:

None - this is the default behavior.

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.)

References:

1. CCE-37942-0

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

2.3.5 Domain controller

This section contains recommendations related to Domain Controllers.

2.3.5.1 (L1) Ensure 'Domain controller: Allow server operators to schedule tasks' is set to 'Disabled' (DC only) (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa: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
```

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.

Default Value:

Disabled. (Server Operators are not allowed to submit jobs by means of the AT schedule facility.)

References:

1. CCE-37848-9

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

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.

4.6 Use of Dedicated Machines For All Administrative Tasks
Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.

2.3.5.2 (L1) Ensure 'Domain controller: LDAP server signing requirements' is set to 'Require signing' (DC only) (Scored)

Profile Applicability:

- Level 1 - 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. For more information on how to identify whether your DCs are being accessed via unsigned LDAP (and where those accesses are coming from), see this Microsoft TechNet blog article: [Identifying Clear Text LDAP binds to your DC's – Practical Windows Security]

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.

Audit:

Navigate to the UI Path articulated in 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\NTDS\Parameters:LDAPServ
erIntegrity
```

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
```

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.

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. CCE-35904-2

CIS Controls:

Version 6

3 Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

2.3.5.3 (L1) Ensure 'Domain controller: Refuse machine account password changes' is set to 'Disabled' (DC only) (Scored)

Profile Applicability:

- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters:Refu
sePasswordChange
```

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
```

Impact:

None - this is the default behavior.

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.)

References:

1. CCE-36921-5

CIS Controls:

Version 6

16 Account Monitoring and Control
Account Monitoring and Control

Version 7

5.1 Establish Secure Configurations
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 (L1) Ensure 'Domain member: Digitally encrypt or sign secure channel data (always)' is set to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters:Requ
ireSignOrSeal
```

Remediation:

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

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

Impact:

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

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

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

Default Value:

Enabled. (All secure channel data must be signed or encrypted.)

References:

1. CCE-36142-8

CIS Controls:

Version 6

13 Data Protection
Data Protection

Version 7

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

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

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

Remediation:

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

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

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.

Default Value:

Enabled. (The domain member will request encryption of all secure channel traffic.)

References:

1. CCE-37130-2

CIS Controls:

Version 6

13 Data Protection
Data Protection

Version 7

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

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

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

Remediation:

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

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

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.

Default Value:

Enabled. (The domain member will request digital signing of all secure channel traffic.)

References:

1. CCE-37222-7

CIS Controls:

Version 6

13 Data Protection
Data Protection

Version 7

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

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters:Disa
blePasswordChange
```

Remediation:

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

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

Impact:

None - this is the default behavior.

Default Value:

Disabled. (The domain member can change its computer account password as specified by the *Domain Member: Maximum machine account password age* setting (Rule 2.3.6.5), which by default is every 30 days.)

References:

1. CCE-37508-9

CIS Controls:

Version 6

16 Account Monitoring and Control
Account Monitoring and Control

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

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 `30 or fewer days, but not 0`:

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

Impact:

None - this is the default behavior.

Default Value:

30 days.

References:

1. CCE-37431-4

CIS Controls:

Version 6

16 Account Monitoring and Control
Account Monitoring and Control

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.)

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters:Requ
ireStrongKey
```

Remediation:

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

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

Impact:

None - this is the default behavior. However, computers will not be able to join Windows NT 4.0 domains, and trusts between Active Directory domains and Windows NT-style domains may not work properly. Also, Domain Controllers with this setting configured will not allow older pre-Windows 2000 clients (that that do not support this policy setting) to join the domain.

Default Value:

Enabled. (The secure channel will not be established unless 128-bit encryption can be performed.)

References:

1. CCE-37614-5

CIS Controls:

Version 6

13 Data Protection
Data Protection

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

2.3.7 Interactive logon

This section contains recommendations related to interactive logons.

2.3.7.1 (L1) Ensure 'Interactive logon: Do not display last user name' is set to 'Enabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

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

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Interactive logon: 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*.

Impact:

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

Default Value:

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

References:

1. CCE-36056-0

CIS Controls:

Version 6

13 Data Protection
Data Protection

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

16.2 Configure Centralized Point of Authentication
Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.

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

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:
DisableCAD
```

Remediation:

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

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

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.

Default Value:

On Windows Server 2008 R2 or older: Disabled.

On Windows Server 2012 (non-R2) or newer: Enabled.

References:

1. CCE-37637-6

CIS Controls:

Version 6

8 Malware Defenses
Malware Defenses

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

16.2 Configure Centralized Point of Authentication
Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:
InactivityTimeoutSecs
```

Remediation:

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

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

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.

Default Value:

0 seconds. (There is no inactivity limit).

References:

1. CCE-38235-8

CIS Controls:

Version 6

16.5 Ensure Workstation Screen Locks Are Configured
Configure screen locks on systems to limit access to unattended workstations.

Version 7

16.11 Lock Workstation Sessions After Inactivity
Automatically lock workstation sessions after a standard period of inactivity.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:
LegalNoticeText
```

Remediation:

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

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

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.

Default Value:

No message.

References:

1. CCE-37226-8

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

16.2 Configure Centralized Point of Authentication
Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:
LegalNoticeCaption
```

Remediation:

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

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

Impact:

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

Default Value:

No message.

References:

1. CCE-37512-1

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

16.2 Configure Centralized Point of Authentication

Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.

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

Profile Applicability:

- Level 2 - 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.

Audit:

Navigate to the UI Path articulated in the 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)
```

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.

Default Value:

On Windows Server 2008 (non-R2): 25 logons.

On Windows Server 2008 R2 or newer: 10 logons.

References:

1. CCE-37439-7

CIS Controls:

Version 6

16 Account Monitoring and Control
Account Monitoring and Control

Version 7

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.

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

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

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon:PasswordExpiryWarning
```

Remediation:

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

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

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.

Default Value:

5 days.

References:

1. CCE-37622-8

CIS Controls:

Version 6

16 Account Monitoring and Control
Account Monitoring and Control

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

16.2 Configure Centralized Point of Authentication
Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.

2.3.7.8 (L1) Ensure 'Interactive logon: Require Domain Controller Authentication to unlock workstation' is set to 'Enabled' (MS only) (Scored)

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.

Audit:

Navigate to the UI Path articulated in the 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: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
```

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.

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.)

References:

1. CCE-38240-8

CIS Controls:

Version 6

16.9 Configure Account Access Centrally
Configure access for all accounts through a centralized point of authentication, for example Active Directory or LDAP. Configure network and security devices for centralized authentication as well.

Version 7

16.2 Configure Centralized Point of Authentication
Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.

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

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.

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
```

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.

Default Value:

No action.

References:

1. CCE-38333-1

CIS Controls:

Version 6

16.5 Ensure Workstation Screen Locks Are Configured
Configure screen locks on systems to limit access to unattended workstations.

Version 7

16.11 Lock Workstation Sessions After Inactivity
Automatically lock workstation sessions after a standard period of inactivity.

2.3.8 Microsoft network client

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

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parame
ters: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)
```

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.

Default Value:

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

References:

1. CCE-36325-9

CIS Controls:

Version 6

13 Data Protection
Data Protection

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parame
ters: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)
```

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.

Default Value:

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

References:

1. CCE-36269-9

CIS Controls:

Version 6

13 Data Protection
Data Protection

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parame
ters: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
```

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.

Default Value:

Disabled. (Plaintext passwords will not be sent during authentication to third-party SMB servers that do not support password encryption.)

References:

1. CCE-37863-8

CIS Controls:

Version 6

13 Data Protection
Data Protection

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

2.3.9 Microsoft network server

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

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

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

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

Remediation:

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

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

Impact:

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

Default Value:

15 minutes.

References:

1. CCE-38046-9

CIS Controls:

Version 6

3 Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

Version 7

16.11 Lock Workstation Sessions After Inactivity
Automatically lock workstation sessions after a standard period of inactivity.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

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

Remediation:

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

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

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.

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.)

References:

1. CCE-37864-6

CIS Controls:

Version 6

13 Data Protection
Data Protection

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

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

Remediation:

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

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

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.

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.)

References:

1. CCE-35988-5

CIS Controls:

Version 6

13 Data Protection
Data Protection

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

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

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

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

Remediation:

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

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

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.

Default Value:

Enabled. (Client sessions with the SMB service are forcibly disconnected when the client's logon hours expire.)

References:

1. CCE-37972-7

CIS Controls:

Version 6

16 Account Monitoring and Control
Account Monitoring and Control

Version 7

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

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

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

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

Remediation:

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

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

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.

Default Value:

Off. (The SPN is not required or validated by the SMB server from a SMB client.)

References:

1. CCE-36170-9

CIS Controls:

Version 6

14 Controlled Access Based on the Need to Know
Controlled Access Based on the Need to Know

Version 7

5.1 Establish Secure Configurations
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 (L1) Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

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

Remediation:

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

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

Impact:

None - this is the default behavior.

Default Value:

Disabled. (An anonymous user cannot request the SID attribute for another user.)

References:

1. CCE-36065-1

CIS Controls:

Version 6

13 Data Protection
Data Protection

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

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

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.)

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa:RestrictAnonymousSAM
```

Remediation:

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

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

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.

Default Value:

Enabled. (Do not allow anonymous enumeration of SAM accounts. This option replaces Everyone with Authenticated Users in the security permissions for resources.)

References:

1. CCE-36316-8

CIS Controls:

Version 6

16 Account Monitoring and Control
Account Monitoring and Control

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

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

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.)

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa:RestrictAnonymous
```

Remediation:

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

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

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`.

Default Value:

Disabled. (Allow anonymous enumeration of SAM accounts and shares. No additional permissions can be assigned by the administrator for anonymous connections to the computer. Anonymous connections will rely on default permissions.)

References:

1. CCE-36077-6

CIS Controls:

Version 6

16 Account Monitoring and Control
Account Monitoring and Control

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

2.3.10.4 (L2) Ensure 'Network access: Do not allow storage of passwords and credentials for network authentication' is set to 'Enabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa:DisableDomainCreds
```

Remediation:

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

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

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.

Default Value:

Disabled. (Credential Manager will store passwords and credentials on the computer for later use for domain authentication.)

References:

1. CCE-38119-4

CIS Controls:

Version 6

16.14 Encrypt/Hash All Authentication Files And Monitor Their Access
Verify that all authentication files are encrypted or hashed and that these files cannot be accessed without root or administrator privileges. Audit all access to password files in the system.

Version 7

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

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa:EveryoneIncludesAnony
mous
```

Remediation:

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

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

Impact:

None - this is the default behavior.

Default Value:

Disabled. (Anonymous users can only access those resources for which the built-in group `ANONYMOUS LOGON` has been explicitly given permission.)

References:

1. CCE-36148-5

CIS Controls:

Version 6

14 Controlled Access Based on the Need to Know
Controlled Access Based on the Need to Know

16 Account Monitoring and Control
Account Monitoring and Control

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

2.3.10.6 (L1) Configure 'Network access: Named Pipes that can be accessed anonymously' (DC only) (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

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

Remediation:

To establish the recommended configuration via GP, 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
```

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.

Default Value:

None.

References:

1. CCE-38258-0

CIS Controls:

Version 6

14.1 Implement Network Segmentation Based On Information Class
Segment the network based on the label or classification level of the information stored on the servers. Locate all sensitive information on separated VLANS with firewall filtering to ensure that only authorized individuals are only able to communicate with systems necessary to fulfill their specific responsibilities.

16 Account Monitoring and Control
Account Monitoring and Control

Version 7

14.1 Segment the Network Based on Sensitivity
Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).

14.2 Enable Firewall Filtering Between VLANs
Enable firewall filtering between VLANs to ensure that only authorized systems are able to communicate with other systems necessary to fulfill their specific responsibilities.

2.3.10.7 (L1) Configure 'Network access: Named Pipes that can be accessed anonymously' (MS only) (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

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

Remediation:

To establish the recommended configuration via GP, 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
```

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.

Default Value:

None.

References:

1. CCE-38258-0

CIS Controls:

Version 6

14.1 Implement Network Segmentation Based On Information Class
Segment the network based on the label or classification level of the information stored on the servers. Locate all sensitive information on separated VLANS with firewall filtering to ensure that only authorized individuals are only able to communicate with systems necessary to fulfill their specific responsibilities.

16 Account Monitoring and Control
Account Monitoring and Control

Version 7

14.1 Segment the Network Based on Sensitivity
Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).

14.2 Enable Firewall Filtering Between VLANs
Enable firewall filtering between VLANs to ensure that only authorized systems are able to communicate with other systems necessary to fulfill their specific responsibilities.

2.3.10.8 (L1) Configure 'Network access: Remotely accessible registry paths' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\Winreg\
AllowedExactPaths:Machine
```

Remediation:

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

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

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.

Default Value:

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

References:

1. CCE-37194-8

CIS Controls:

Version 6

14 Controlled Access Based on the Need to Know
Controlled Access Based on the Need to Know

14.6 Enforce Detailed Audit Logging For Sensitive Information
Enforce detailed audit logging for access to nonpublic data and special authentication for sensitive data.

16 Account Monitoring and Control
Account Monitoring and Control

Version 7

14.9 Enforce Detail Logging for Access or Changes to Sensitive Data
Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).

2.3.10.9 (L1) Configure 'Network access: Remotely accessible registry paths and sub-paths' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\Winreg\
AllowedPaths:Machine
```

Remediation:

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

```
System\CurrentControlSet\Control\Print\Printers
System\CurrentControlSet\Services\Eventlog
Software\Microsoft\OLAP Server
Software\Microsoft\Windows NT\CurrentVersion\Print
Software\Microsoft\Windows NT\CurrentVersion\Windows
System\CurrentControlSet\Control\ContentIndex
System\CurrentControlSet\Control\Terminal Server
System\CurrentControlSet\Control\Terminal Server\UserConfig
System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration
Software\Microsoft\Windows NT\CurrentVersion\Perflib
System\CurrentControlSet\Services\SysmonLog
```

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

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`

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.

Default Value:

System\CurrentControlSet\Control\Print\Printers
System\CurrentControlSet\Services\Eventlog
Software\Microsoft\OLAP Server
Software\Microsoft\Windows NT\CurrentVersion\Print
Software\Microsoft\Windows NT\CurrentVersion\Windows
System\CurrentControlSet\Control\ContentIndex
System\CurrentControlSet\Control\Terminal Server
System\CurrentControlSet\Control\Terminal Server\UserConfig
System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration
Software\Microsoft\Windows NT\CurrentVersion\Perflib
System\CurrentControlSet\Services\SysmonLog

References:

1. CCE-36347-3

CIS Controls:

Version 6

14 Controlled Access Based on the Need to Know
Controlled Access Based on the Need to Know

16 Account Monitoring and Control
Account Monitoring and Control

Version 7

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.

14.9 Enforce Detail Logging for Access or Changes to Sensitive Data
Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

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

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network access: Restrict anonymous access to Named
Pipes and Shares
```

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.

Default Value:

Enabled. (Anonymous access is restricted to shares and pipes listed in the `Network access: Named pipes that can be accessed anonymously` and `Network access: Shares that can be accessed anonymously` settings.)

References:

1. CCE-36021-4

CIS Controls:

Version 6

14 Controlled Access Based on the Need to Know
Controlled Access Based on the Need to Know

16 Account Monitoring and Control
Account Monitoring and Control

Version 7

14.6 Protect Information through Access Control Lists
Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

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

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

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

Remediation:

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

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

Impact:

None - this is the default behavior.

Default Value:

None. (Only authenticated users will have access to all shared resources on the server.)

References:

1. CCE-38095-6

CIS Controls:

Version 6

14 Controlled Access Based on the Need to Know
Controlled Access Based on the Need to Know

16 Account Monitoring and Control
Account Monitoring and Control

Version 7

14.6 Protect Information through Access Control Lists
Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

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

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa:ForceGuest
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Classic - local users authenticate as themselves`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network access: Sharing and security model for
local accounts
```

Impact:

None - this is the default configuration for domain-joined computers.

Default Value:

On domain-joined computers: Classic - local users authenticate as themselves. (Network logons that use local account credentials authenticate by using those credentials.)

On stand-alone computers: Guest only - local users authenticate as Guest. (Network logons that use local accounts are automatically mapped to the Guest account.)

References:

1. CCE-37623-6

CIS Controls:

Version 6

14 Controlled Access Based on the Need to Know
Controlled Access Based on the Need to Know

16 Account Monitoring and Control
Account Monitoring and Control

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

2.3.11 Network security

This section contains recommendations related to network security.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa:UseMachineId
```

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network security: Allow Local System to use
computer identity for NTLM
```

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.

Default Value:

Disabled. (Services running as Local System that use Negotiate when reverting to NTLM authentication will authenticate anonymously.)

References:

1. CCE-38341-4

CIS Controls:

Version 6

14 Controlled Access Based on the Need to Know
Controlled Access Based on the Need to Know

16 Account Monitoring and Control
Account Monitoring and Control

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

16.2 Configure Centralized Point of Authentication
Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0:AllowNullSessi
onFallback
```

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network security: Allow LocalSystem NULL session
fallback
```

Impact:

Any applications that require NULL sessions for LocalSystem will not work as designed.

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

References:

1. CCE-37035-3

CIS Controls:

Version 6

14 Controlled Access Based on the Need to Know
Controlled Access Based on the Need to Know

Version 7

16.2 Configure Centralized Point of Authentication
Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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`.

Rationale:

The PKU2U protocol is a peer-to-peer authentication protocol - authentication should be managed centrally in most managed networks.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\pku2u:AllowOnlineID
```

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network Security: Allow PKU2U authentication
requests to this computer to use online identities
```

Impact:

None - this is the default configuration for domain-joined computers.

Default Value:

Disabled. (Online identities will not to be allowed to authenticate to a domain-joined machine.)

References:

1. CCE-38047-7

CIS Controls:

Version 6

16.9 Configure Account Access Centrally
Configure access for all accounts through a centralized point of authentication, for example Active Directory or LDAP. Configure network and security devices for centralized authentication as well.

Version 7

16.2 Configure Centralized Point of Authentication
Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.

2.3.11.4 (L1) Ensure 'Network security: Configure encryption types allowed for Kerberos' is set to 'AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.`

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\
Kerberos\Parameters:SupportedEncryptionTypes
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network security: Configure encryption types
allowed for Kerberos
```

Impact:

If not selected, the encryption type will not be allowed. This setting may affect compatibility with client computers or services and applications. Multiple selections are permitted.

Note: Some legacy applications and OSes may require `RC4_HMAC_MD5` - we recommend you test in your environment and verify whether you can safely remove it.

Note #2: Windows Server 2008 (non-R2) and below allow DES for Kerberos by default, but later OS versions do not.

Default Value:

RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types.

References:

1. CCE-37755-6

CIS Controls:

Version 6

16.14 Encrypt/Hash All Authentication Files And Monitor Their Access
Verify that all authentication files are encrypted or hashed and that these files cannot be accessed without root or administrator privileges. Audit all access to password files in the system.

Version 7

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

16.5 Encrypt Transmittal of Username and Authentication Credentials
Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa:NoLMHash
```

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network security: Do not store LAN Manager hash
value on next password change
```

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.

Default Value:

Enabled. (LAN Manager hash values are not stored when passwords are changed.)

References:

1. CCE-36326-7

CIS Controls:

Version 6

16.14 Encrypt/Hash All Authentication Files And Monitor Their Access
Verify that all authentication files are encrypted or hashed and that these files cannot be accessed without root or administrator privileges. Audit all access to password files in the system.

Version 7

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

16.5 Encrypt Transmittal of Username and Authentication Credentials
Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.

2.3.11.6 (L1) Ensure 'Network security: Force logoff when logon hours expire' is set to 'Enabled' (Not Scored)

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.

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
```

Impact:

None - this is the default behavior.

Default Value:

Enabled. (When a user's logon time expires, client sessions with the SMB server will be forcibly disconnected. The user will be unable to log on to the computer until their next scheduled access time commences.)

References:

1. CCE-36270-7

CIS Controls:

Version 6

16 Account Monitoring and Control
Account Monitoring and Control

Version 7

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

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa:LmCompatibilityLevel
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to: `Send NTLMv2 response only. Refuse LM & NTLM`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network security: LAN Manager authentication level
```

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.

Default Value:

Send NTLMv2 response only. (Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it; Domain Controllers accept LM, NTLM & NTLMv2 authentication.)

References:

1. CCE-36173-3

CIS Controls:

Version 6

13 Data Protection
Data Protection

Version 7

16.2 Configure Centralized Point of Authentication
Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LDAP:LDAPClientIntegrity
```

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network security: LDAP client signing requirements
```

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.

Default Value:

Negotiate signing. (If Transport Layer Security/Secure Sockets Layer (TLS/SSL) has not been started, the LDAP BIND request is initiated with the LDAP data signing option set in addition to the caller-specified options. If TLS/SSL has been started, the LDAP BIND request is initiated with the caller-specified options.)

References:

1. CCE-36858-9

CIS Controls:

Version 6

13 Data Protection
Data Protection

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

2.3.11.9 (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit encryption' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0: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
```

Impact:

NTLM connections will fail if NTLMv2 protocol and strong encryption (128-bit) are not **both** negotiated. Client applications that are enforcing these settings will be unable to communicate with older servers that do not support them. This setting could impact Windows Clustering when applied to servers running Windows Server 2003, see Microsoft Knowledge Base article 890761: You receive an "Error 0x8007042b" error message when you add or join a node to a cluster if you use NTLM version 2 in Windows Server 2003 for more information on possible issues and how to resolve them.

Default Value:

On Windows Server 2008 (non-R2): No requirements.

On Windows Server 2008 R2 and newer: Require 128-bit encryption. (NTLM connections will fail if strong encryption (128-bit) is not negotiated.)

References:

1. CCE-37553-5

CIS Controls:

Version 6

13 Data Protection
Data Protection

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

2.3.11.10 (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0: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
```

Impact:

NTLM connections will fail if NTLMv2 protocol and strong encryption (128-bit) are not **both** negotiated. Server applications that are enforcing these settings will be unable to communicate with older servers that do not support them. This setting could impact Windows Clustering when applied to servers running Windows Server 2003, see Microsoft Knowledge Base article 890761: You receive an "Error 0x8007042b" error message when you add or join a node to a cluster if you use NTLM version 2 in Windows Server 2003 for more information on possible issues and how to resolve them.

Default Value:

On Windows Server 2008 (non-R2): No requirements.

On Windows Server 2008 R2 and newer: Require 128-bit encryption. (NTLM connections will fail if strong encryption (128-bit) is not negotiated.)

References:

1. CCE-37835-6

CIS Controls:

Version 6

13 Data Protection
Data Protection

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

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 (L1) Ensure 'Shutdown: Allow system to be shut down without having to log on' is set to 'Disabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

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

Impact:

None - this is the default behavior.

Default Value:

Disabled. (Operators will have to log on to servers to shut them down or restart them.)

References:

1. CCE-36788-8

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

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.

4.6 Use of Dedicated Machines For All Administrative Tasks

Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.

2.3.14 System cryptography

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

2.3.15 System objects

This section contains recommendations related to system objects.

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

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session
Manager\Kernel:ObCaseInsensitive
```

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\System objects: Require case insensitivity for non-
Windows subsystems
```

Impact:

None - this is the default behavior.

Default Value:

Enabled. (All subsystems will be forced to observe case insensitivity. This configuration may confuse users who are familiar with any UNIX-based operating systems that is case-sensitive.)

References:

1. CCE-37885-1

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session
Manager:ProtectionMode
```

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\System objects: Strengthen default permissions of
internal system objects (e.g. Symbolic Links)
```

Impact:

None - this is the default behavior.

Default Value:

Enabled. (The default DACL is stronger, allowing users who are not administrators to read shared objects but not allowing these users to modify shared objects that they did not create.)

References:

1. CCE-37644-2

CIS Controls:

Version 6

14.4 Protect Information With Access Control Lists
All information stored on systems shall be protected 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.

Version 7

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.

2.3.16 System settings

This section contains recommendations related to system settings.

2.3.16.1 (L1) Ensure 'System settings: Optional subsystems' is set to 'Defined: (blank)' (Scored)

Profile Applicability:

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

Description:

This security setting determines which subsystems can optionally be started up to support your applications. With this security setting, you can specify as many subsystems to support your applications as your environment demands.

The recommended state for this setting is: `Defined: (blank)`

Rationale:

POSIX is included with Windows and enabled by default. If you don't need it, leaving it enabled could introduce an additional attack surface to your environment.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session
Manager\SubSystems:Optional
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Defined: (blank)`:

```
Computer Configuration\Security Settings\Local Policies\Security
Options\System settings: Optional subsystems
```

Impact:

Removes POSIX compatibility.

Default Value:

POSIX.

References:

1. CCE-35921-6

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

2.3.17 User Account Control

This section contains recommendations related to User Account Control.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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 and newer, the built-in Administrator account is now disabled by default. In a default installation of a new computer, accounts with administrative control over the computer are initially set up in one of two ways:

- If the computer is not joined to a domain, the first user account you create has the equivalent permissions as a local administrator.
- If the computer is joined to a domain, no local administrator accounts are created. The Enterprise or Domain Administrator must log on to the computer and create one if a local administrator account is warranted.

Once Windows is installed, the built-in Administrator account may be manually enabled, but we strongly recommend that this account remain disabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:
FilterAdministratorToken
```

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\User Account Control: Admin Approval Mode for the
Built-in Administrator account
```

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.

Default Value:

Disabled. (The built-in Administrator account runs all applications with full administrative privilege.)

References:

1. CCE-36494-3

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

4.4 Use Unique Passwords

Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.

2.3.17.2 (L1) Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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`.

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:
ConsentPromptBehaviorAdmin
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Prompt for consent on the secure desktop`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\User Account Control: Behavior of the elevation
prompt for administrators in Admin Approval Mode
```

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.

Default Value:

Prompt for consent for non-Windows binaries. (When an operation for a non-Microsoft application requires elevation of privilege, the user is prompted on the secure desktop to select either Permit or Deny. If the user selects Permit, the operation continues with the user's highest available privilege.)

References:

1. CCE-37029-6

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

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.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:
ConsentPromptBehaviorUser
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Automatically deny elevation requests`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\User Account Control: Behavior of the elevation
prompt for standard users
```

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.

Default Value:

Prompt for credentials. (When an operation requires elevation of privilege, the user is prompted to enter an administrative user name and password. If the user enters valid credentials, the operation continues with the applicable privilege.)

References:

1. CCE-36864-7

CIS Controls:

Version 6

5.1 <u>Minimize And Sparingly Use Administrative Privileges</u>
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

5.1 <u>Establish Secure Configurations</u>
Maintain documented, standard security configuration standards for all authorized operating systems and software.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

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

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\User Account Control: Detect application
installations and prompt for elevation
```

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.

Default Value:

Disabled. (Default for enterprise. Application installation packages are not detected and prompted for elevation.)

References:

1. CCE-36533-8

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

2.6 Address unapproved software
Ensure that unauthorized software is either removed or the inventory is updated in a timely manner

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.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:
EnableSecureUIAPaths
```

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\User Account Control: Only elevate UIAccess
applications that are installed in secure locations
```

Impact:

None - this is the default behavior.

Default Value:

Enabled. (If an application resides in a secure location in the file system, it runs only with UIAccess integrity.)

References:

1. CCE-37057-7

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

16.2 Configure Centralized Point of Authentication
Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:
EnableLUA
```

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\User Account Control: Run all administrators in
Admin Approval Mode
```

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.

Default Value:

Enabled. (Admin Approval Mode is enabled. This policy must be enabled and related UAC policy settings must also be set appropriately to allow the built-in Administrator account and all other users who are members of the Administrators group to run in Admin Approval Mode.)

References:

1. CCE-36869-6

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

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.

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

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

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

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\User Account Control: Switch to the secure desktop
when prompting for elevation
```

Impact:

None - this is the default behavior.

Default Value:

Enabled. (All elevation requests go to the secure desktop regardless of prompt behavior policy settings for administrators and standard users.)

References:

1. CCE-36866-2

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

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.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:
EnableVirtualization
```

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\User Account Control: Virtualize file and registry
write failures to per-user locations
```

Impact:

None - this is the default behavior.

Default Value:

Enabled. (Application write failures are redirected at run time to defined user locations for both the file system and registry.)

References:

1. CCE-37064-3

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

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

6 Registry

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

7 File System

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

8 Wired Network (IEEE 802.3) Policies

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

9 Windows Firewall with Advanced Security

This section contains recommendations for configuring the Windows Firewall.

9.1 Domain Profile

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

9.1.1 (L1) Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\
EnableFirewall
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `On (recommended)`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Domain Profile\Firewall state
```

Impact:

None - this is the default behavior.

Default Value:

On (recommended). (The Windows Firewall with Advanced Security will be active in this profile.)

References:

1. CCE-36062-8

CIS Controls:

Version 6

9.2 Leverage Host-based Firewalls
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.

Version 7

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.

11.1 Maintain Standard Security Configurations for Network Devices
Maintain standard, documented security configuration standards for all authorized network devices.

11.2 Document Traffic Configuration Rules
All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.

11.3 Use Automated Tools to Verify Standard Device Configurations and Detect Changes
Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.

9.1.2 (L1) Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\
DefaultInboundAction
```

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Domain Profile\Inbound connections
```

Impact:

None - this is the default behavior.

Default Value:

Block (default). (The Windows Firewall with Advanced Security will block all inbound connections that do not match an inbound firewall rule in this profile.)

References:

1. CCE-38117-8

CIS Controls:

Version 6

9.2 Leverage Host-based Firewalls
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.

Version 7

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.

11.2 Document Traffic Configuration Rules
All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.

11.3 Use Automated Tools to Verify Standard Device Configurations and Detect Changes
Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.

9.1.3 (L1) Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\
DefaultOutboundAction
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Allow (default)`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Domain Profile\Outbound connections
```

Impact:

None - this is the default behavior.

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.)

References:

1. CCE-36146-9

CIS Controls:

Version 6

9.2 Leverage Host-based Firewalls
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.

Version 7

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.

11.2 Document Traffic Configuration Rules
All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.

11.3 Use Automated Tools to Verify Standard Device Configurations and Detect Changes
Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.

9.1.4 (L1) Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\
DisableNotifications
```

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Domain Profile\Settings
Customize\Display a notification
```

Impact:

Windows Firewall will not display a notification when a program is blocked from receiving inbound connections.

Default Value:

Yes. (Windows Firewall with Advanced Security will display a notification when a program is blocked from receiving inbound connections.)

References:

1. CCE-38041-0

CIS Controls:

Version 7

11.2 Document Traffic Configuration Rules

All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.

11.3 Use Automated Tools to Verify Standard Device Configurations and Detect Changes

Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.

9.1.5 (L1) Ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\domainfw.log' (Scored)

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 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\
Logging\LogFilePath
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `%SystemRoot%\System32\logfiles\firewall\domainfw.log`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Domain Profile\Logging Customize\Name
```

Impact:

The log file will be stored in the specified file.

Default Value:

`%SystemRoot%\System32\logfiles\firewall\pfirewall.log`

References:

1. CCE-37482-7

CIS Controls:

Version 6

6.2 Ensure Audit Log Settings Support Appropriate Log Entry Formatting

Validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction. Systems should record logs in a standardized format such as syslog entries or those outlined by the Common Event Expression initiative. If systems cannot generate logs in a standardized format, log normalization tools can be deployed to convert logs into such a format.

Version 7

6.2 Activate audit logging

Ensure that local logging has been enabled on all systems and networking devices.

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

6.5 Central Log Management

Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.

9.1.6 (L1) Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\
Logging\LogFileSize
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `16,384 KB or greater`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Domain Profile\Logging Customize\Size
limit (KB)
```

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.

Default Value:

4,096 KB.

References:

1. CCE-36088-3

CIS Controls:

Version 6

6.3 Ensure Audit Logging Systems Are Not Subject To Loss (i.e. rotation/archive)
Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals. The logs must be archived and digitally signed on a periodic basis.

Version 7

6.4 Ensure adequate storage for logs
Ensure that all systems that store logs have adequate storage space for the logs generated.

6.5 Central Log Management
Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.

9.1.7 (L1) Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\
Logging\LogDroppedPackets
```

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Domain Profile\Logging Customize\Log
dropped packets
```

Impact:

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

Default Value:

No (default). (Information about dropped packets will not be recorded in the firewall log file.)

References:

1. CCE-37523-8

CIS Controls:

Version 6

6.2 Ensure Audit Log Settings Support Appropriate Log Entry Formatting
Validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction. Systems should record logs in a standardized format such as syslog entries or those outlined by the Common Event Expression initiative. If systems cannot generate logs in a standardized format, log normalization tools can be deployed to convert logs into such a format.

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

6.3 Enable Detailed Logging
Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

6.5 Central Log Management
Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.

9.1.8 (L1) Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\
Logging\LogSuccessfulConnections
```

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Domain Profile\Logging Customize\Log
successful connections
```

Impact:

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

Default Value:

No (default). (Information about successful connections will not be recorded in the firewall log file.)

References:

1. CCE-36393-7

CIS Controls:

Version 6

6.2 Ensure Audit Log Settings Support Appropriate Log Entry Formatting
Validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction. Systems should record logs in a standardized format such as syslog entries or those outlined by the Common Event Expression initiative. If systems cannot generate logs in a standardized format, log normalization tools can be deployed to convert logs into such a format.

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

6.3 Enable Detailed Logging
Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

6.5 Central Log Management
Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.

9.2 Private Profile

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

9.2.1 (L1) Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile
:EnableFirewall
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `On (recommended)`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Private Profile\Firewall state
```

Impact:

None - this is the default behavior.

Default Value:

On (recommended). (The Windows Firewall with Advanced Security will be active in this profile.)

References:

1. CCE-38239-0

CIS Controls:

Version 6

9.2 Leverage Host-based Firewalls
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.

Version 7

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.

11.2 Document Traffic Configuration Rules
All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.

11.3 Use Automated Tools to Verify Standard Device Configurations and Detect Changes
Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.

9.2.2 (L1) Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile
:DefaultInboundAction
```

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Private Profile\Inbound connections
```

Impact:

None - this is the default behavior.

Default Value:

Block (default). (The Windows Firewall with Advanced Security will block all inbound connections that do not match an inbound firewall rule in this profile.)

References:

1. CCE-38042-8

CIS Controls:

Version 6

9.2 Leverage Host-based Firewalls
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.

Version 7

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.

11.2 Document Traffic Configuration Rules
All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.

11.3 Use Automated Tools to Verify Standard Device Configurations and Detect Changes
Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.

9.2.3 (L1) Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile
:DefaultOutboundAction
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Allow (default)`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Private Profile\Outbound connections
```

Impact:

None - this is the default behavior.

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.)

References:

1. CCE-38332-3

CIS Controls:

Version 6

9.2 Leverage Host-based Firewalls
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.

Version 7

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.

11.2 Document Traffic Configuration Rules
All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.

11.3 Use Automated Tools to Verify Standard Device Configurations and Detect Changes
Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.

9.2.4 (L1) Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile
:DisableNotifications
```

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Private Profile\Settings
Customize\Display a notification
```

Impact:

Windows Firewall will not display a notification when a program is blocked from receiving inbound connections.

Default Value:

Yes. (Windows Firewall with Advanced Security will display a notification when a program is blocked from receiving inbound connections.)

References:

1. CCE-37621-0

CIS Controls:

Version 7

11.2 Document Traffic Configuration Rules

All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.

11.3 Use Automated Tools to Verify Standard Device Configurations and Detect Changes

Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.

9.2.5 (L1) Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\privatefw.log' (Scored)

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 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile
\Logging:LogFilePath
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `%SystemRoot%\System32\logfiles\firewall\privatefw.log`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Private Profile\Logging Customize\Name
```

Impact:

The log file will be stored in the specified file.

Default Value:

`%SystemRoot%\System32\logfiles\firewall\pfirewall.log`

References:

1. CCE-37569-1

CIS Controls:

Version 6

6.2 Ensure Audit Log Settings Support Appropriate Log Entry Formatting

Validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction. Systems should record logs in a standardized format such as syslog entries or those outlined by the Common Event Expression initiative. If systems cannot generate logs in a standardized format, log normalization tools can be deployed to convert logs into such a format.

Version 7

6.2 Activate audit logging

Ensure that local logging has been enabled on all systems and networking devices.

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

6.5 Central Log Management

Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.

9.2.6 (L1) Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile
\Logging:LogFileSize
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `16,384 KB or greater`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Private Profile\Logging Customize\Size
limit (KB)
```

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.

Default Value:

4,096 KB.

References:

1. CCE-38178-0

CIS Controls:

Version 6

6.3 Ensure Audit Logging Systems Are Not Subject To Loss (i.e. rotation/archive)
Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals. The logs must be archived and digitally signed on a periodic basis.

Version 7

6.4 Ensure adequate storage for logs
Ensure that all systems that store logs have adequate storage space for the logs generated.

6.5 Central Log Management
Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.

9.2.7 (L1) Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile
\Logging:LogDroppedPackets
```

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Private Profile\Logging Customize\Log
dropped packets
```

Impact:

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

Default Value:

No (default). (Information about dropped packets will not be recorded in the firewall log file.)

References:

1. CCE-35972-9

CIS Controls:

Version 6

6.2 Ensure Audit Log Settings Support Appropriate Log Entry Formatting

Validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction. Systems should record logs in a standardized format such as syslog entries or those outlined by the Common Event Expression initiative. If systems cannot generate logs in a standardized format, log normalization tools can be deployed to convert logs into such a format.

Version 7

6.2 Activate audit logging

Ensure that local logging has been enabled on all systems and networking devices.

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

6.5 Central Log Management

Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.

9.2.8 (L1) Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile
\Logging:LogSuccessfulConnections
```

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Private Profile\Logging Customize\Log
successful connections
```

Impact:

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

Default Value:

No (default). (Information about successful connections will not be recorded in the firewall log file.)

References:

1. CCE-37387-8

CIS Controls:

Version 6

6.2 Ensure Audit Log Settings Support Appropriate Log Entry Formatting

Validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction. Systems should record logs in a standardized format such as syslog entries or those outlined by the Common Event Expression initiative. If systems cannot generate logs in a standardized format, log normalization tools can be deployed to convert logs into such a format.

Version 7

6.2 Activate audit logging

Ensure that local logging has been enabled on all systems and networking devices.

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

6.5 Central Log Management

Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.

9.3 Public Profile

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

9.3.1 (L1) Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile:
EnableFirewall
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `On (recommended)`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Public Profile\Firewall state
```

Impact:

None - this is the default behavior.

Default Value:

On (recommended). (The Windows Firewall with Advanced Security will be active in this profile.)

References:

1. CCE-37862-0

CIS Controls:

Version 6

9.2 Leverage Host-based Firewalls
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.

Version 7

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.

11.2 Document Traffic Configuration Rules
All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.

11.3 Use Automated Tools to Verify Standard Device Configurations and Detect Changes
Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.

9.3.2 (L1) Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile:
DefaultInboundAction
```

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Public Profile\Inbound connections
```

Impact:

None - this is the default behavior.

Default Value:

Block (default). (The Windows Firewall with Advanced Security will block all inbound connections that do not match an inbound firewall rule in this profile.)

References:

1. CCE-36057-8

CIS Controls:

Version 6

9.2 Leverage Host-based Firewalls
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.

Version 7

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.

11.2 Document Traffic Configuration Rules
All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.

11.3 Use Automated Tools to Verify Standard Device Configurations and Detect Changes
Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.

9.3.3 (L1) Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile:
DefaultOutboundAction
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Allow (default)`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Public Profile\Outbound connections
```

Impact:

None - this is the default behavior.

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.)

References:

1. CCE-37434-8

CIS Controls:

Version 6

9.2 Leverage Host-based Firewalls
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.

Version 7

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.

11.2 Document Traffic Configuration Rules
All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.

11.3 Use Automated Tools to Verify Standard Device Configurations and Detect Changes
Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.

9.3.4 (L1) Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'No' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile:
DisableNotifications
```

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Public Profile\Settings
Customize\Display a notification
```

Impact:

Windows Firewall will not display a notification when a program is blocked from receiving inbound connections.

Default Value:

Yes. (Windows Firewall with Advanced Security will display a notification when a program is blocked from receiving inbound connections.)

References:

1. CCE-38043-6

CIS Controls:

Version 7

11.2 Document Traffic Configuration Rules

All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.

11.3 Use Automated Tools to Verify Standard Device Configurations and Detect Changes

Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.

9.3.5 (L1) Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile:
AllowLocalPolicyMerge
```

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Public Profile\Settings Customize\Apply
local firewall rules
```

Impact:

Administrators can still create firewall rules, but the rules will not be applied.

Default Value:

Yes (default). (Firewall rules created by administrators will be applied.)

References:

1. CCE-37861-2

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

11.2 Document Traffic Configuration Rules

All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.

11.3 Use Automated Tools to Verify Standard Device Configurations and Detect Changes

Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.

9.3.6 (L1) Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile:
AllowLocalIPsecPolicyMerge
```

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Public Profile\Settings Customize\Apply
local connection security rules
```

Impact:

Administrators can still create local connection security rules, but the rules will not be applied.

Default Value:

Yes (default). (Local connection security rules created by administrators will be applied.)

References:

1. CCE-36268-1

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

11.2 Document Traffic Configuration Rules

All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.

11.3 Use Automated Tools to Verify Standard Device Configurations and Detect Changes

Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.

9.3.7 (L1) Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\publicfw.log' (Scored)

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 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile\
Logging:LogFilePath
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `%SystemRoot%\System32\logfiles\firewall\publicfw.log`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Public Profile\Logging Customize\Name
```

Impact:

The log file will be stored in the specified file.

Default Value:

`%SystemRoot%\System32\logfiles\firewall\pfirewall.log`

References:

1. CCE-37266-4

CIS Controls:

Version 6

6.2 Ensure Audit Log Settings Support Appropriate Log Entry Formatting

Validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction. Systems should record logs in a standardized format such as syslog entries or those outlined by the Common Event Expression initiative. If systems cannot generate logs in a standardized format, log normalization tools can be deployed to convert logs into such a format.

Version 7

6.2 Activate audit logging

Ensure that local logging has been enabled on all systems and networking devices.

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

6.5 Central Log Management

Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.

9.3.8 (L1) Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile\
Logging:LogFileSize
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `16,384 KB or greater`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Public Profile\Logging Customize\Size
limit (KB)
```

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.

Default Value:

4,096 KB.

References:

1. CCE-36395-2

CIS Controls:

Version 6

6.3 Ensure Audit Logging Systems Are Not Subject To Loss (i.e. rotation/archive)
Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals. The logs must be archived and digitally signed on a periodic basis.

Version 7

6.4 Ensure adequate storage for logs
Ensure that all systems that store logs have adequate storage space for the logs generated.

6.5 Central Log Management
Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.

9.3.9 (L1) Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile\
Logging:LogDroppedPackets
```

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Public Profile\Logging Customize\Log
dropped packets
```

Impact:

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

Default Value:

No (default). (Information about dropped packets will not be recorded in the firewall log file.)

References:

1. CCE-37265-6

CIS Controls:

Version 6

6.2 Ensure Audit Log Settings Support Appropriate Log Entry Formatting
Validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction. Systems should record logs in a standardized format such as syslog entries or those outlined by the Common Event Expression initiative. If systems cannot generate logs in a standardized format, log normalization tools can be deployed to convert logs into such a format.

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

6.3 Enable Detailed Logging
Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

6.5 Central Log Management
Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.

9.3.10 (L1) Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile\
Logging:LogSuccessfulConnections
```

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Public Profile\Logging Customize\Log
successful connections
```

Impact:

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

Default Value:

No (default). (Information about successful connections will not be recorded in the firewall log file.)

References:

1. CCE-36394-5

CIS Controls:

Version 6

6.2 Ensure Audit Log Settings Support Appropriate Log Entry Formatting
Validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction. Systems should record logs in a standardized format such as syslog entries or those outlined by the Common Event Expression initiative. If systems cannot generate logs in a standardized format, log normalization tools can be deployed to convert logs into such a format.

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

6.3 Enable Detailed Logging
Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

6.5 Central Log Management
Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.

10 Network List Manager Policies

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

11 Wireless Network (IEEE 802.11) Policies

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

12 Public Key Policies

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

13 Software Restriction Policies

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

14 Network Access Protection NAP Client Configuration

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

15 Application Control Policies

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

16 IP Security Policies

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

17 Advanced Audit Policy Configuration

This section contains recommendations for configuring the Windows audit facilities.

17.1 Account Logon

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

17.1.1 (L1) Ensure 'Audit Credential Validation' is set to 'Success and Failure' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

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

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Account Logon\Audit Credential
Validation
```

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.

Default Value:

Success.

References:

1. CCE-37741-6

CIS Controls:

Version 6

16.12 Use Long Passwords For All User Accounts

Where multi-factor authentication is not supported, user accounts shall be required to use long passwords on the system (longer than 14 characters).

16.4 Automatically Log Off Users After Standard Period Of Inactivity

Regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.

16.8 Log Attempts To Access Deactivated Accounts

Monitor attempts to access deactivated accounts through audit logging.

Version 7

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.

16.12 Monitor Attempts to Access Deactivated Accounts

Monitor attempts to access deactivated accounts through audit logging.

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.

16.9 Disable Dormant Accounts

Automatically disable dormant accounts after a set period of inactivity.

17.1.2 (L1) Ensure 'Audit Kerberos Authentication Service' is set to 'Success and Failure' (DC Only) (Scored)

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.

Audit:

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

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Account Logon\Audit Kerberos
Authentication Service
```

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.

Default Value:

Success.

References:

1. CCE-38140-0

CIS Controls:

Version 6

16.4 Automatically Log Off Users After Standard Period Of Inactivity
Regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.

16.8 Log Attempts To Access Deactivated Accounts
Monitor attempts to access deactivated accounts through audit logging.

Version 7

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.

16.12 Monitor Attempts to Access Deactivated Accounts
Monitor attempts to access deactivated accounts through audit logging.

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.

16.9 Disable Dormant Accounts
Automatically disable dormant accounts after a set period of inactivity.

17.1.3 (L1) Ensure 'Audit Kerberos Service Ticket Operations' is set to 'Success and Failure' (DC Only) (Scored)

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.

Audit:

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

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Account Logon\Audit Kerberos
Service Ticket Operations
```

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.

Default Value:

Success.

References:

1. CCE-37975-0

CIS Controls:

Version 7

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.

16.12 Monitor Attempts to Access Deactivated Accounts
Monitor attempts to access deactivated accounts through audit logging.

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.

16.9 Disable Dormant Accounts
Automatically disable dormant accounts after a set period of inactivity.

17.2 Account Management

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

17.2.1 (L1) Ensure 'Audit Application Group Management' is set to 'Success and Failure' (Scored)

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`.

Rationale:

Auditing events in this category may be useful when investigating an incident.

Audit:

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

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Account Management\Audit
Application Group Management
```

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.

Default Value:

No Auditing.

References:

1. CCE-38329-9

CIS Controls:

Version 6

16 Account Monitoring and Control
Account Monitoring and Control

Version 7

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.

16.12 Monitor Attempts to Access Deactivated Accounts
Monitor attempts to access deactivated accounts through audit logging.

16.9 Disable Dormant Accounts
Automatically disable dormant accounts after a set period of inactivity.

17.2.2 (L1) Ensure 'Audit Computer Account Management' is set to include 'Success' (DC only) (Scored)

Profile Applicability:

- Level 1 - 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.

Audit:

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

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Account Management\Audit Computer
Account Management
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

Success.

References:

1. CCE-38004-8

CIS Controls:

Version 6

1 Inventory of Authorized and Unauthorized Devices
Inventory of Authorized and Unauthorized Devices

Version 7

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.

17.2.3 (L1) Ensure 'Audit Distribution Group Management' is set to include 'Success' (DC only) (Scored)

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.

Audit:

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

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Account Management\Audit
Distribution Group Management
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

No Auditing.

References:

1. CCE-36265-7

CIS Controls:

Version 6

16 Account Monitoring and Control
Account Monitoring and Control

Version 7

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.

16.6 Maintain an Inventory of Accounts
Maintain an inventory of all accounts organized by authentication system.

17.2.4 (L1) Ensure 'Audit Other Account Management Events' is set to include 'Success' (DC only) (Scored)

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.

Audit:

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

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Account Management\Audit Other
Account Management Events
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

No Auditing.

References:

1. CCE-37855-4

CIS Controls:

Version 6

16.4 Automatically Log Off Users After Standard Period Of Inactivity
Regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.

Version 7

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.

16.6 Maintain an Inventory of Accounts
Maintain an inventory of all accounts organized by authentication system.

17.2.5 (L1) Ensure 'Audit Security Group Management' is set to include 'Success' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

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

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Account Management\Audit Security
Group Management
```

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.

Default Value:

Success.

References:

1. CCE-38034-5

CIS Controls:

Version 6

16 Account Monitoring and Control
Account Monitoring and Control

Version 7

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.

16.6 Maintain an Inventory of Accounts
Maintain an inventory of all accounts organized by authentication system.

17.2.6 (L1) Ensure 'Audit User Account Management' is set to 'Success and Failure' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

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

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Account Management\Audit User
Account Management
```

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.

Default Value:

Success.

References:

1. CCE-37856-2

CIS Controls:

Version 6

16.4 Automatically Log Off Users After Standard Period Of Inactivity
Regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.

Version 7

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.

16.6 Maintain an Inventory of Accounts
Maintain an inventory of all accounts organized by authentication system.

17.3 Detailed Tracking

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

17.3.1 (L1) Ensure 'Audit Process Creation' is set to include 'Success' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

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

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Detailed Tracking\Audit Process
Creation
```

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.

Default Value:

No Auditing.

References:

1. CCE-36059-4

CIS Controls:

Version 7

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 (L1) Ensure 'Audit Directory Service Access' is set to include 'Failure' (DC only) (Scored)

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.

Audit:

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

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\DS Access\Audit Directory Service
Access
```

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.

Default Value:

Success.

References:

1. CCE-37433-0

CIS Controls:

Version 6

14.4 Protect Information With Access Control Lists
All information stored on systems shall be protected 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.

Version 7

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.

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.

17.4.2 (L1) Ensure 'Audit Directory Service Changes' is set to include 'Success' (DC only) (Scored)

Profile Applicability:

- Level 1 - 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.

Audit:

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

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\DS Access\Audit Directory Service
Changes
```

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.

Default Value:

No Auditing.

References:

1. CCE-37616-0

CIS Controls:

Version 6

14.4 Protect Information With Access Control Lists
All information stored on systems shall be protected 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.

Version 7

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.

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.

17.5 Logon/Logoff

This section contains recommendations for configuring the Logon/Logoff audit policy.

17.5.1 (L1) Ensure 'Audit Account Lockout' is set to include 'Failure' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

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

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Account Lockout
```

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.

Default Value:

Success.

References:

1. CCE-37133-6

CIS Controls:

Version 6

16.7 Configure Account Lockouts
Use and configure account lockouts such that after a set number of failed login attempts the account is locked for a standard period of time.

Version 7

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.

16.6 Maintain an Inventory of Accounts
Maintain an inventory of all accounts organized by authentication system.

17.5.2 (L1) Ensure 'Audit Logoff' is set to include 'Success' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

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

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Logoff
```

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.

Default Value:

Success.

References:

1. CCE-38237-4

CIS Controls:

Version 6

16.10 Profile User Account Usage And Monitor For Anomalies
Profile each user's typical account usage by determining normal time-of-day access and access duration. Reports should be generated that indicate users who have logged in during unusual hours or have exceeded their normal login duration. This includes flagging the use of the user's credentials from a computer other than computers on which the user generally works.

Version 7

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.

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.

16.6 Maintain an Inventory of Accounts
Maintain an inventory of all accounts organized by authentication system.

17.5.3 (L1) Ensure 'Audit Logon' is set to 'Success and Failure' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

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

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Logon
```

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.

Default Value:

Success and Failure.

References:

1. CCE-38036-0

CIS Controls:

Version 6

16.10 Profile User Account Usage And Monitor For Anomalies

Profile each user's typical account usage by determining normal time-of-day access and access duration. Reports should be generated that indicate users who have logged in during unusual hours or have exceeded their normal login duration. This includes flagging the use of the user's credentials from a computer other than computers on which the user generally works.

Version 7

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.

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.

16.6 Maintain an Inventory of Accounts

Maintain an inventory of all accounts organized by authentication system.

17.5.4 (L1) Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure' (Scored)

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.

Audit:

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

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Other
Logon/Logoff Events
```

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.

Default Value:

No Auditing.

References:

1. CCE-36322-6

CIS Controls:

Version 6

16.10 Profile User Account Usage And Monitor For Anomalies

Profile each user's typical account usage by determining normal time-of-day access and access duration. Reports should be generated that indicate users who have logged in during unusual hours or have exceeded their normal login duration. This includes flagging the use of the user's credentials from a computer other than computers on which the user generally works.

Version 7

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.

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.

16.6 Maintain an Inventory of Accounts

Maintain an inventory of all accounts organized by authentication system.

17.5.5 (L1) Ensure 'Audit Special Logon' is set to include 'Success' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

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

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Special Logon
```

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.

Default Value:

Success.

References:

1. CCE-36266-5

CIS Controls:

Version 6

5.8 Administrators Should Not Directly Log In To A System (i.e. use RunAs/sudo)
Administrators should be required to access a system using a fully logged and non-administrative account. Then, once logged on to the machine without administrative privileges, the administrator should transition to administrative privileges using tools such as Sudo on Linux/UNIX, RunAs on Windows, and other similar facilities for other types of systems.

Version 7

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.

16.6 Maintain an Inventory of Accounts
Maintain an inventory of all accounts organized by authentication system.

17.6 Object Access

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

17.6.1 (L1) Ensure 'Audit Detailed File Share' is set to include 'Failure' (Scored)

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.

Audit:

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

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Object Access\Audit Detailed File
Share
```

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.

Default Value:

No Auditing.

References:

1. CCE-36878-7

CIS Controls:

Version 7

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.

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

17.6.2 (L1) Ensure 'Audit File Share' is set to 'Success and Failure' (Scored)

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.

Audit:

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

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Object Access\Audit File Share
```

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.

Default Value:

No Auditing.

References:

1. CCE-37384-5

CIS Controls:

Version 6

14.4 Protect Information With Access Control Lists
All information stored on systems shall be protected 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.

Version 7

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.

14.6 Protect Information through Access Control Lists
Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

17.6.3 (L1) Ensure 'Audit Other Object Access Events' is set to 'Success and Failure' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

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

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Object Access\Audit Other Object
Access Events
```

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.

Default Value:

No Auditing.

References:

1. CCE-37620-2

CIS Controls:

Version 6

6.2 Ensure Audit Log Settings Support Appropriate Log Entry Formatting

Validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction. Systems should record logs in a standardized format such as syslog entries or those outlined by the Common Event Expression initiative. If systems cannot generate logs in a standardized format, log normalization tools can be deployed to convert logs into such a format.

Version 7

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

17.6.4 (L1) Ensure 'Audit Removable Storage' is set to 'Success and Failure' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

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

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Object Access\Audit Removable
Storage
```

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.

Default Value:

No Auditing.

References:

1. CCE-37617-8

CIS Controls:

Version 6

8.3 Limit Use Of External Devices (i.e. USB)

Limit use of external devices to those with an approved, documented business need. Monitor for use and attempted use of external devices. Configure laptops, workstations, and servers so that they will not auto-run content from removable media, like USB tokens (i.e., "thumb drives"), USB hard drives, CDs/DVDs, FireWire devices, external serial advanced technology attachment devices, and mounted network shares. Configure systems so that they automatically conduct an anti-malware scan of removable media when inserted.

Version 7

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.

8.4 Configure Anti-Malware Scanning of Removable Devices

Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.

8.5 Configure Devices Not To Auto-run Content

Configure devices to not auto-run content from removable media.

13.8 Manage System's External Removable Media's Read/write Configurations

Configure systems not to write data to external removable media, if there is no business need for supporting such devices.

17.7 Policy Change

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

17.7.1 (L1) Ensure 'Audit Audit Policy Change' is set to include 'Success' (Scored)

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.

Audit:

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

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Policy Change\Audit Audit Policy
Change
```

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.

Default Value:

Success.

References:

1. CCE-38028-7

CIS Controls:

Version 6

3.5 Use File Integrity Tools For Critical System Files

Use file integrity checking tools to ensure that critical system files (including sensitive system and application executables, libraries, and configurations) have not been altered. The reporting system should: have the ability to account for routine and expected changes; highlight and alert on unusual or unexpected alterations; show the history of configuration changes over time and identify who made the change (including the original logged-in account in the event of a user ID switch, such as with the su or sudo command). These integrity checks should identify suspicious system alterations such as: owner and permissions changes to files or directories; the use of alternate data streams which could be used to hide malicious activities; and the introduction of extra files into key system areas (which could indicate malicious payloads left by attackers or additional files inappropriately added during batch distribution processes).

Version 7

5.5 Implement Automated Configuration Monitoring Systems

Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.

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.

14.9 Enforce Detail Logging for Access or Changes to Sensitive Data

Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).

17.7.2 (L1) Ensure 'Audit Authentication Policy Change' is set to include 'Success' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

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

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Policy Change\Audit Authentication
Policy Change
```

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.

Default Value:

Success.

References:

1. CCE-38327-3

CIS Controls:

Version 6

3.5 Use File Integrity Tools For Critical System Files

Use file integrity checking tools to ensure that critical system files (including sensitive system and application executables, libraries, and configurations) have not been altered. The reporting system should: have the ability to account for routine and expected changes; highlight and alert on unusual or unexpected alterations; show the history of configuration changes over time and identify who made the change (including the original logged-in account in the event of a user ID switch, such as with the su or sudo command). These integrity checks should identify suspicious system alterations such as: owner and permissions changes to files or directories; the use of alternate data streams which could be used to hide malicious activities; and the introduction of extra files into key system areas (which could indicate malicious payloads left by attackers or additional files inappropriately added during batch distribution processes).

Version 7

5.5 Implement Automated Configuration Monitoring Systems

Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.

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.

14.9 Enforce Detail Logging for Access or Changes to Sensitive Data

Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).

17.7.3 (L1) Ensure 'Audit Authorization Policy Change' is set to include 'Success' (Scored)

Profile Applicability:

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

Description:

This subcategory reports changes in authorization policy. Events for this subcategory include:

- 4704: A user right was assigned.
- 4705: A user right was removed.
- 4706: A new trust was created to a domain.
- 4707: A trust to a domain was removed.
- 4714: Encrypted data recovery policy was changed.

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

Rationale:

Auditing these events may be useful when investigating a security incident.

Audit:

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

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Policy Change\Audit Authorization
Policy Change
```

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.

Default Value:

Success.

References:

1. CCE-36320-0

CIS Controls:

Version 6

3.5 Use File Integrity Tools For Critical System Files

Use file integrity checking tools to ensure that critical system files (including sensitive system and application executables, libraries, and configurations) have not been altered. The reporting system should: have the ability to account for routine and expected changes; highlight and alert on unusual or unexpected alterations; show the history of configuration changes over time and identify who made the change (including the original logged-in account in the event of a user ID switch, such as with the su or sudo command). These integrity checks should identify suspicious system alterations such as: owner and permissions changes to files or directories; the use of alternate data streams which could be used to hide malicious activities; and the introduction of extra files into key system areas (which could indicate malicious payloads left by attackers or additional files inappropriately added during batch distribution processes).

Version 7

5.5 Implement Automated Configuration Monitoring Systems

Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.

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.

14.9 Enforce Detail Logging for Access or Changes to Sensitive Data

Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).

17.7.4 (L1) Ensure 'Audit MPSSVC Rule-Level Policy Change' is set to 'Success and Failure' (Scored)

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.

Audit:

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

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Policy Change\Audit MPSSVC Rule-
Level Policy Change
```

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.

Default Value:

No Auditing.

References:

1. CCE-37852-1

CIS Controls:

Version 7

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.

17.7.5 (L1) Ensure 'Audit Other Policy Change Events' is set to include 'Failure' (Scored)

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.

Audit:

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

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Policy Change\Audit Other Policy
Change Events
```

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.

Default Value:

No Auditing.

References:

1. CCE-38029-5

CIS Controls:

Version 7

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

17.8 Privilege Use

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

17.8.1 (L1) Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

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

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Privilege Use\Audit Sensitive
Privilege Use
```

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.

Default Value:

No Auditing.

References:

1. CCE-36267-3

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

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.

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

17.9 System

This section contains recommendations for configuring the System audit policy.

17.9.1 (L1) Ensure 'Audit IPsec Driver' is set to 'Success and Failure' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

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

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\System\Audit IPsec Driver
```

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.

Default Value:

No Auditing.

References:

1. CCE-37853-9

CIS Controls:

Version 6

13 Data Protection
Data Protection

Version 7

6.3 Enable Detailed Logging
Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

6.4 Ensure adequate storage for logs
Ensure that all systems that store logs have adequate storage space for the logs generated.

6.5 Central Log Management
Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.

17.9.2 (L1) Ensure 'Audit Other System Events' is set to 'Success and Failure' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

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

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\System\Audit Other System Events
```

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.

Default Value:

Success and Failure.

References:

1. CCE-38030-3

CIS Controls:

Version 6

9.2 Leverage Host-based Firewalls

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.

Version 7

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

6.4 Ensure adequate storage for logs

Ensure that all systems that store logs have adequate storage space for the logs generated.

6.5 Central Log Management

Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.

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.

17.9.3 (L1) Ensure 'Audit Security State Change' is set to include 'Success' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

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

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\System\Audit Security State Change
```

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.

Default Value:

Success.

References:

1. CCE-38114-5

CIS Controls:

Version 7

6.3 Enable Detailed Logging
Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

6.4 Ensure adequate storage for logs
Ensure that all systems that store logs have adequate storage space for the logs generated.

6.5 Central Log Management
Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.

17.9.4 (L1) Ensure 'Audit Security System Extension' is set to include 'Success' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

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

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\System\Audit Security System
Extension
```

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.

Default Value:

No Auditing.

References:

1. CCE-36144-4

CIS Controls:

Version 6

6 Maintenance, Monitoring, and Analysis of Audit Logs
Maintenance, Monitoring, and Analysis of Audit Logs

Version 7

6.3 Enable Detailed Logging
Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

6.4 Ensure adequate storage for logs
Ensure that all systems that store logs have adequate storage space for the logs generated.

6.5 Central Log Management
Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.

17.9.5 (L1) Ensure 'Audit System Integrity' is set to 'Success and Failure' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

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

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\System\Audit System Integrity
```

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.

Default Value:

Success and Failure.

References:

1. CCE-37132-8

CIS Controls:

Version 6

6 Maintenance, Monitoring, and Analysis of Audit Logs
Maintenance, Monitoring, and Analysis of Audit Logs

Version 7

6.3 Enable Detailed Logging
Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

6.4 Ensure adequate storage for logs
Ensure that all systems that store logs have adequate storage space for the logs generated.

6.5 Central Log Management
Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.

18 Administrative Templates (Computer)

This section contains computer-based recommendations from Group Policy Administrative Templates (ADMX).

18.1 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.

18.2 LAPS

This section contains recommendations for configuring Microsoft Local Administrator Password Solution (LAPS).

This Group Policy section is provided by the Group Policy template `AdmPwd.admx/adml` that is included with LAPS.

18.2.1 (L1) Ensure LAPS AdmPwd GPO Extension / CSE is installed (MS only) (Scored)

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.

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.

Audit:

The LAPS AdmPwd GPO Extension / CSE can be verified to be installed by the presence of the following registry value:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon\GPExtensions\{D76B9641-3288-4f75-942D-
087DE603E3EA}:DllName
```

Remediation:

In order to utilize LAPS, a minor Active Directory Schema update is required, and a Group Policy Client Side Extension (CSE) must be installed on each managed computer. When LAPS is installed, the file `AdmPwd.dll` must be present in the following location and registered in Windows (the LAPS AdmPwd GPO Extension / CSE installation does this for you):

```
C:\Program Files\LAPS\CSE\AdmPwd.dll
```

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.

Default Value:

Not Installed.

CIS Controls:

Version 6

16.9 Configure Account Access Centrally

Configure access for all accounts through a centralized point of authentication, for example Active Directory or LDAP. Configure network and security devices for centralized authentication as well.

Version 7

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.

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.

18.2.2 (L1) Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled' (MS only) (Scored)

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.

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft
Services\AdmPwd:PwdExpirationProtectionEnabled
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\LAPS\Do not allow
password expiration time longer than required by policy
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`AdmPwd.admx/adml`) is required - it is included with Microsoft Local Administrator Password Solution (LAPS).

Impact:

Planned password expiration longer than password age dictated by "Password Settings" policy is NOT allowed.

Default Value:

Disabled. (Password expiration time may be longer than required by the "Password Settings" policy.)

CIS Controls:

Version 6

16.2 All Accounts Have A Monitored Expiration Date
Ensure that all accounts have an expiration date that is monitored and enforced.

Version 7

16.10 Ensure All Accounts Have An Expiration Date
Ensure that all accounts have an expiration date that is monitored and enforced.

18.2.3 (L1) Ensure 'Enable Local Admin Password Management' is set to 'Enabled' (MS only) (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft Services\AdmPwd:AdmPwdEnabled
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\LAPS\Enable Local
Admin Password Management
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`AdmPwd.admx/adml`) is required - it is included with Microsoft Local Administrator Password Solution (LAPS).

Impact:

The local administrator password is managed (provided that the LAPS AdmPwd GPO Extension / CSE is installed on the target computer (see Rule 18.2.1), the Active Directory domain schema and account permissions have been properly configured on the domain).

In a disaster recovery scenario where Active Directory is not available, the local Administrator password will not be retrievable and a local password reset using a tool (such as Microsoft's Disaster and Recovery Toolset (DaRT) Recovery Image) may be necessary.

Default Value:

Disabled. (Local Administrator password is NOT managed.)

CIS Controls:

Version 6

16.9 Configure Account Access Centrally

Configure access for all accounts through a centralized point of authentication, for example Active Directory or LDAP. Configure network and security devices for centralized authentication as well.

Version 7

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.

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.

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

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft
Services\AdmPwd:PasswordComplexity
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`, and configure the `Password Complexity` option to `Large letters + small letters + numbers + special characters`:

```
Computer Configuration\Policies\Administrative Templates\LAPS\Password
Settings
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`AdmPwd.admx/adml`) is required - it is included with Microsoft Local Administrator Password Solution (LAPS).

Impact:

LAPS-generated passwords will be required to contain large letters + small letters + numbers + special characters.

Default Value:

Large letters + small letters + numbers + special characters.

CIS Controls:

Version 6

5.7 User Accounts Shall Use Long Passwords

Where multi-factor authentication is not supported, user accounts shall be required to use long passwords on the system (longer than 14 characters).

Version 7

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.

18.2.5 (L1) Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more' (MS only) (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft Services\AdmPwd:PasswordLength
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`, and configure the `Password Length` option to `15 or more`:

```
Computer Configuration\Policies\Administrative Templates\LAPS\Password
Settings
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`AdmPwd.admx/adml`) is required - it is included with Microsoft Local Administrator Password Solution (LAPS).

Impact:

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

Default Value:

14 characters.

CIS Controls:

Version 6

5.7 User Accounts Shall Use Long Passwords

Where multi-factor authentication is not supported, user accounts shall be required to use long passwords on the system (longer than 14 characters).

Version 7

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.

18.2.6 (L1) Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer' (MS only) (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft
Services\AdmPwd:PasswordAgeDays
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`, and configure the `Password Age (Days)` option to `30 or fewer`:

```
Computer Configuration\Policies\Administrative Templates\LAPS\Password
Settings
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`AdmPwd.admx/adml`) is required - it is included with Microsoft Local Administrator Password Solution (LAPS).

Impact:

LAPS-generated passwords will be required to have a maximum age of 30 days (or fewer, if selected).

Default Value:

30 days.

CIS Controls:

Version 6

16.5 Ensure Workstation Screen Locks Are Configured
Configure screen locks on systems to limit access to unattended workstations.

Version 7

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 MS Security Guide

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

This Group Policy section is provided by the Group Policy template `SecGuide.admx/adml` that is available from Microsoft at this link.

18.3.1 (L1) Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled' (MS only) (Scored)

Profile Applicability:

- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

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

Remediation:

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

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

Note: This Group Policy path does not exist by default. An additional Group Policy template (`SecGuide.admx/adml`) is required - it is available from Microsoft at this link.

Impact:

None - this is the default behavior.

Default Value:

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

References:

1. CCE-37069-2

CIS Controls:

Version 6

5.8 Administrators Should Not Directly Log In To A System (i.e. use RunAs/sudo)

Administrators should be required to access a system using a fully logged and non-administrative account. Then, once logged on to the machine without administrative privileges, the administrator should transition to administrative privileges using tools such as Sudo on Linux/UNIX, RunAs on Windows, and other similar facilities for other types of systems.

Version 7

4.3 Ensure the Use of Dedicated Administrative Accounts

Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.

18.3.2 (L1) Ensure 'Configure SMB v1 client' is set to 'Enabled: Bowser, MRxSmb20, NSI' (Scored)

Profile Applicability:

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

Description:

This setting configures the dependencies for the Lanman Workstation service - since disabling the Server Message Block version 1 (SMBv1) protocol is recommended, therefore the `MRxSmb10` dependency, which is used only by SMBv1, should no longer be configured.

The recommended state for this setting is: `Enabled: Bowser, MRxSmb20, NSI.`

Note: Do not, *under any circumstances*, configure this setting as `Disabled`, as doing so will delete the underlying registry entry altogether, which will cause serious problems.

Rationale:

Since September 2016, Microsoft has strongly encouraged that SMBv1 be disabled and no longer used on modern networks, as it is a 30 year old design that is much more vulnerable to attacks then much newer designs such as SMBv2 and SMBv3.

More information on this can be found at the following links:

Stop using SMB1 | Storage at Microsoft

Disable SMB v1 in Managed Environments with Group Policy – "Stay Safe" Cyber Security Blog

Disabling SMBv1 through Group Policy – Microsoft Security Guidance blog

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation:Depend
OnService
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Bowser, MRxSmb20, NSI`:

```
Computer Configuration\Policies\Administrative Templates\MS Security Guide\Configure SMB v1 client
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`SecGuide.admx/adml`) is required - it is available from Microsoft at this link.

Impact:

Some legacy OSes (e.g. Windows XP, Server 2003 or older), applications and appliances may no longer be able to communicate with the system once SMBv1 is disabled. We recommend careful testing be performed to determine the impact prior to configuring this as a widespread control, where possible, remediate any incompatibilities found. Microsoft is also maintaining a thorough (although not comprehensive) list of known SMBv1 incompatibilities at this link: SMB1 Product Clearinghouse | Storage at Microsoft

Default Value:

Windows Server 2012 (non-R2) and older: Enabled: Bowser, MRxSmb10, MRxSmb20, NSI

Windows Server 2012 R2 and newer: Enabled: Bowser, MRxSmb20, NSI

CIS Controls:

Version 6

9.1 Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

9.3 Perform Regular Automated Port Scans
Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.

18.3.3 (L1) Ensure 'Configure SMB v1 client driver' is set to 'Enabled: Disable driver (recommended)' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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 then much newer designs such as SMBv2 and SMBv3.

More information on this can be found at the following links:

Stop using SMB1 | Storage at Microsoft

Disable SMB v1 in Managed Environments with Group Policy – "Stay Safe" Cyber Security Blog

Disabling SMBv1 through Group Policy – Microsoft Security Guidance blog

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\mrxsmb10:Start
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\MS Security Guide\Configure SMB v1 client driver
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`SecGuide.admx/adml`) is required - it is available from Microsoft at this link.

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

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 and newer: Enabled: Disable driver.

CIS Controls:

Version 6

9.1 Limit Open Ports, Protocols, and Services

Ensure that only ports, protocols, and services with validated business needs are running on each system.

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

9.3 Perform Regular Automated Port Scans

Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.

18.3.4 (L1) Ensure 'Configure SMB v1 server' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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 then much newer designs such as SMBv2 and SMBv3.

More information on this can be found at the following links:

Stop using SMB1 | Storage at Microsoft

Disable SMB v1 in Managed Environments with Group Policy – "Stay Safe" Cyber Security Blog

Disabling SMBv1 through Group Policy – Microsoft Security Guidance blog

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters:
SMB1
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\MS Security
Guide\Configure SMB v1 server
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`SecGuide.admx/adml`) is required - it is available from Microsoft at this link.

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

Default Value:

Windows Server 2016 R1607 and older: Enabled.

Windows Server 2016 R1709 and newer: Disabled.

CIS Controls:

Version 6

9.1 Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

9.3 Perform Regular Automated Port Scans
Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.

18.3.5 (L1) Ensure 'Enable Structured Exception Handling Overwrite Protection (SEHOP)' is set to 'Enabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session
Manager\kernel:DisableExceptionChainValidation
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\MS Security
Guide\Enable Structured Exception Handling Overwrite Protection (SEHOP)
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`SecGuide.admx/adml`) is required - it is available from Microsoft at this link.
More information is available at MSKB 956607: How to enable Structured Exception Handling Overwrite Protection (SEHOP) in Windows operating systems

Impact:

After you enable SEHOP, existing versions of Cygwin, Skype, and Armadillo-protected applications may not work correctly.

Default Value:

Disabled for 32-bit processes.

CIS Controls:

Version 6

8.4 Enable Anti-exploitation Features (i.e. DEP, ASLR, EMET)

Enable anti-exploitation features such as Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualization/containerization, etc. For increased protection, deploy capabilities such as Enhanced Mitigation Experience Toolkit (EMET) that can be configured to apply these protections to a broader set of applications and executables.

Version 7

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.

18.3.6 (L1) Ensure 'Extended Protection for LDAP Authentication (Domain Controllers only)' is set to 'Enabled: Enabled, always (recommended)' (DC Only) (Scored)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This setting controls LDAP authentication over SSL/TLS to help make it more secure.

The recommended state for this setting is: `Enabled: Enabled, always (recommended)`.

Note: All LDAP clients must have the CVC-2017-8563 security update to be compatible with Domain Controllers that have this setting enabled.

Note #2: In March 2020, Microsoft added a new GPO setting named *Domain controller: LDAP server channel binding token requirements* which was bundled with that month's Windows security patches. This new "native" setting configures the exact same `LdapEnforceChannelBinding` registry value and does not depend on an ADMX template. Therefore it should be considered a "superseding" method of achieving the same results. However, since Extended Support ended on January 14, 2020 for Windows Server 2008 (non-R2) and Windows Server 2008 R2, and they are no longer receiving security patches (unless hosted on Azure or under a paid support contract), they typically do not have the March 2020 (or later) patch readily available. If this is the case in your environment, this ADMX-based setting should be used with those OSes instead of the new native setting.

More information on this setting is available at: Use the LdapEnforceChannelBinding registry entry to make LDAP authentication over SSL-TLS more secure

Rationale:

Configuring the LdapEnforceChannelBinding registry value can help to increase protection against "man-in-the-middle" attacks.

Audit:

Navigate to the UI Path articulated in 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\NTDS\Parameters:LdapEnfo
rceChannelBinding
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\MS Security
Guide\Extended Protection for LDAP Authentication (Domain Controllers only)
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`SecGuide.admx/adml`) is required - it is available from Microsoft at this link.

Impact:

All LDAP clients must provide channel binding information. The server 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 Domain Controllers 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 `Enabled: Enabled, when supported` (instead of `Enabled: Enabled, always (recommended)`) 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 `Enabled: Enabled, always (recommended)`, and test each of the critical LDAP clients against that DC (and remediating as necessary), before deploying `Enabled: Enabled, always (recommended)` to the rest of the DCs.

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 `Enabled: Enabled, always (recommended)` is actually considered compliant to the CIS benchmark.

More information on this setting is available at: Use the LdapEnforceChannelBinding registry entry to make LDAP authentication over SSL-TLS more secure

Default Value:

Disabled. (No LDAP channel binding validation is performed.)

CIS Controls:

Version 7

16.5 Encrypt Transmittal of Username and Authentication Credentials

Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.

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

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters:NodeTyp
e
```

Remediation:

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

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

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

Impact:

NetBIOS name resolution queries will require a defined and available WINS server for external NetBIOS name resolution. If a WINS server is not defined or not reachable, and the desired hostname is not defined in the local cache, local LMHOSTS or HOSTS files, NetBIOS name resolution will fail.

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:

Version 6

9 Limitation and Control of Network Ports, Protocols, and Services
Limitation and Control of Network Ports, Protocols, and Services

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

9.3 Perform Regular Automated Port Scans
Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.

18.3.8 (L1) Ensure 'WDigest Authentication' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

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

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\MS Security
Guide\WDigest Authentication (disabling may require KB2871997)
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`SecGuide.admx/adml`) is required - it is available from Microsoft at this link.

Impact:

None - this is also the default configuration for Server 2012 R2 and newer.

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

References:

1. CCE-38444-6

CIS Controls:

Version 6

16.14 Encrypt/Hash All Authentication Files And Monitor Their Access
Verify that all authentication files are encrypted or hashed and that these files cannot be accessed without root or administrator privileges. Audit all access to password files in the system.

Version 7

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

18.4 MSS (Legacy)

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

This Group Policy section is provided by the Group Policy template `MSS-legacy.admx/adml` that is available from this TechNet blog post: [The MSS settings – Microsoft Security Guidance blog]

18.4.1 (L1) Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon:AutoAdminLogon
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS:
(AutoAdminLogon) Enable Automatic Logon (not recommended)
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`MSS-legacy.admx/adml`) is required - it is available from this TechNet blog post: [The MSS settings – Microsoft Security Guidance blog]

Impact:

None - this is the default behavior.

Default Value:

Disabled.

References:

1. CCE-37067-6

CIS Controls:

Version 6

16 Account Monitoring and Control
Account Monitoring and Control

Version 7

4.3 Ensure the Use of Dedicated Administrative Accounts
Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.

18.4.2 (L1) Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters:Disabl
eIPSourceRouting
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Highest protection, source routing is completely disabled`:

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

Note: This Group Policy path does not exist by default. An additional Group Policy template (`MSS-legacy.admx/adml`) is required - it is available from this TechNet blog post: [The MSS settings – Microsoft Security Guidance blog]

Impact:

All incoming source routed packets will be dropped.

Default Value:

No additional protection, source routed packets are allowed.

References:

1. CCE-36871-2

CIS Controls:

Version 6

9 Limitation and Control of Network Ports, Protocols, and Services
Limitation and Control of Network Ports, Protocols, and Services

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

9.3 Perform Regular Automated Port Scans
Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.

18.4.3 (L1) Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters:Disable
IPSourceRouting
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Highest protection, source routing is completely disabled`:

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

Note: This Group Policy path does not exist by default. An additional Group Policy template (`MSS-legacy.admx/adml`) is required - it is available from this TechNet blog post: [The MSS settings – Microsoft Security Guidance blog]

Impact:

All incoming source routed packets will be dropped.

Default Value:

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

References:

1. CCE-36535-3

CIS Controls:

Version 6

9 Limitation and Control of Network Ports, Protocols, and Services
Limitation and Control of Network Ports, Protocols, and Services

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

9.3 Perform Regular Automated Port Scans
Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.

18.4.4 (L1) Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed for your organization. This group policy object is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters:EnableI
CMPRedirect
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS:
(EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`MSS-legacy.admx/adml`) is required - it is available from this TechNet blog post: [The MSS settings – Microsoft Security Guidance blog]

Impact:

When Routing and Remote Access Service (RRAS) is configured as an autonomous system boundary router (ASBR), it does not correctly import connected interface subnet routes. Instead, this router injects host routes into the OSPF routes. However, the OSPF router cannot be used as an ASBR router, and when connected interface subnet routes are imported into OSPF the result is confusing routing tables with strange routing paths.

Default Value:

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

References:

1. CCE-37988-3

CIS Controls:

Version 6

9 Limitation and Control of Network Ports, Protocols, and Services
Limitation and Control of Network Ports, Protocols, and Services

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

9.3 Perform Regular Automated Port Scans
Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.

18.4.5 (L2) Ensure 'MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds' is set to 'Enabled: 300,000 or 5 minutes (recommended)' (Scored)

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 (recommended)`.

Rationale:

An attacker who is able to connect to network applications could establish numerous connections to cause a DoS condition.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters:KeepAli
veTime
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 300,000 or 5 minutes (recommended)`:

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

Note: This Group Policy path does not exist by default. An additional Group Policy template (`MSS-legacy.admx/adml`) is required - it is available from this TechNet blog post: [The MSS settings – Microsoft Security Guidance blog]

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.

Default Value:

7,200,000 milliseconds or 120 minutes.

References:

1. CCE-36868-8

CIS Controls:

Version 6

9 Limitation and Control of Network Ports, Protocols, and Services
Limitation and Control of Network Ports, Protocols, and Services

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

9.3 Perform Regular Automated Port Scans
Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.

18.4.6 (L1) Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters:NoNameR
eleaseOnDemand
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS:
(NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release
requests except from WINS servers
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`MSS-legacy.admx/adml`) is required - it is available from this TechNet blog post: [The MSS settings – Microsoft Security Guidance blog]

Impact:

None - this is the default behavior.

Default Value:

Enabled.

References:

1. CCE-36879-5

CIS Controls:

Version 6

9 Limitation and Control of Network Ports, Protocols, and Services
Limitation and Control of Network Ports, Protocols, and Services

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

9.3 Perform Regular Automated Port Scans
Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.

18.4.7 (L2) Ensure 'MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)' is set to 'Disabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters:Perform
RouterDiscovery
```

Remediation:

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

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

Note: This Group Policy path does not exist by default. An additional Group Policy template (`MSS-legacy.admx/adml`) is required - it is available from this TechNet blog post: [The MSS settings – Microsoft Security Guidance blog]

Impact:

Windows will not automatically detect and configure default gateway addresses on the computer.

Default Value:

Enable only if DHCP sends the Perform Router Discovery option.

References:

1. CCE-38065-9

CIS Controls:

Version 6

9 Limitation and Control of Network Ports, Protocols, and Services
Limitation and Control of Network Ports, Protocols, and Services

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

9.3 Perform Regular Automated Port Scans
Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.

18.4.8 (L1) Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session
Manager:SafeDllSearchMode
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS:
(SafeDllSearchMode) Enable Safe DLL search mode (recommended)
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`MSS-legacy.admx/adml`) is required - it is available from this TechNet blog post: [The MSS settings – Microsoft Security Guidance blog]

Impact:

None - this is the default behavior.

Default Value:

Enabled.

References:

1. CCE-36351-5

CIS Controls:

Version 6

8 Malware Defenses
Malware Defenses

Version 7

8.1 Utilize Centrally Managed Anti-malware Software
Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.

8.2 Ensure Anti-Malware Software and Signatures are Updated
Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.

18.4.9 (L1) Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)' is set to 'Enabled: 5 or fewer seconds' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon:ScreenSaverGracePeriod
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 5 or fewer seconds`:

```
Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS:
(ScreenSaverGracePeriod) The time in seconds before the screen saver grace
period expires (0 recommended)
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`MSS-legacy.admx/adml`) is required - it is available from this TechNet blog post: [The MSS settings – Microsoft Security Guidance blog]

Impact:

Users will have to enter their passwords to resume their console sessions as soon as the grace period ends after screen saver activation.

Default Value:

5 seconds.

References:

1. CCE-37993-3

CIS Controls:

Version 6

16.5 Ensure Workstation Screen Locks Are Configured
Configure screen locks on systems to limit access to unattended workstations.

Version 7

16.11 Lock Workstation Sessions After Inactivity
Automatically lock workstation sessions after a standard period of inactivity.

18.4.10 (L2) Ensure 'MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TCPIP6\Parameters:TcpMax
DataRetransmissions
```

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]

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.

Default Value:

5 times.

References:

1. CCE-37846-3

CIS Controls:

Version 6

9 Limitation and Control of Network Ports, Protocols, and Services
Limitation and Control of Network Ports, Protocols, and Services

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

9.3 Perform Regular Automated Port Scans
Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.

18.4.11 (L2) Ensure 'MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters:TcpMaxD
ataRetransmissions
```

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]

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.

Default Value:

5 times.

References:

1. CCE-36051-1

CIS Controls:

Version 6

9 Limitation and Control of Network Ports, Protocols, and Services
Limitation and Control of Network Ports, Protocols, and Services

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

9.3 Perform Regular Automated Port Scans
Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.

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

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security:Warnin
gLevel
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 90% or less:`

```
Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS:
(WarningLevel) Percentage threshold for the security event log at which the
system will generate a warning
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`MSS-legacy.admx/adml`) is required - it is available from this TechNet blog post: [The MSS settings – Microsoft Security Guidance blog]

Impact:

An audit event will be generated when the Security log reaches the 90% percent full threshold (or whatever lower value may be set) unless the log is configured to overwrite events as needed.

Default Value:

0%. (No warning event is generated.)

References:

1. CCE-36880-3

CIS Controls:

Version 6

6.3 Ensure Audit Logging Systems Are Not Subject To Loss (i.e. rotation/archive)

Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals. The logs must be archived and digitally signed on a periodic basis.

Version 7

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

6.4 Ensure adequate storage for logs

Ensure that all systems that store logs have adequate storage space for the logs generated.

6.5 Central Log Management

Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.

18.5 Network

This section contains recommendations for network settings.

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

18.5.1 Background Intelligent Transfer Service (BITS)

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

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

18.5.2 BranchCache

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

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

18.5.3 DirectAccess Client Experience Settings

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

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

18.5.4 DNS Client

This section contains recommendations related to DNS Client.

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

18.5.4.1 (L1) Ensure 'Turn off multicast name resolution' is set to 'Enabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows
NT\DNSClient:EnableMulticast
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Network\DNS
Client\Turn off multicast name resolution
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `DnsClient.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Impact:

In the event DNS is unavailable a system will be unable to request it from other systems on the same subnet.

Default Value:

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

References:

1. CCE-37450-4

CIS Controls:

Version 6

9 Limitation and Control of Network Ports, Protocols, and Services
Limitation and Control of Network Ports, Protocols, and Services

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

9.3 Perform Regular Automated Port Scans
Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.

18.5.5 Fonts

This section is 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 Release 1607 & Server 2016 Administrative Templates (or newer).

18.5.6 Hotspot Authentication

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

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

18.5.7 Lanman Server

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

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

18.5.8 Lanman Workstation

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

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

18.5.9 Link-Layer Topology Discovery

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

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

18.5.9.1 (L2) Ensure 'Turn on Mapper I/O (LLTDIO) driver' is set to 'Disabled' (Scored)

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.

Audit:

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

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\LLTD:AllowLLTDIOOnDoma
in
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\LLTD:AllowLLTDIOOnPubl
icNet
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\LLTD:EnableLLTDIO
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\LLTD:ProhibitLLTDIOOnP
rivateNet
```

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.

Impact:

None - this is the default behavior.

Default Value:

Disabled. (The Mapper I/O (LLTDIO) network protocol driver is turned off.)

References:

1. CCE-38170-7

CIS Controls:

Version 6

9 Limitation and Control of Network Ports, Protocols, and Services
Limitation and Control of Network Ports, Protocols, and Services

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

9.3 Perform Regular Automated Port Scans
Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.

18.5.9.2 (L2) Ensure 'Turn on Responder (RSPNDR) driver' is set to 'Disabled' (Scored)

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.

Audit:

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

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\LLTD:AllowRspndrOnDoma
in
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\LLTD:AllowRspndrOnPubl
icNet
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\LLTD:EnableRspndr
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\LLTD:ProhibitRspndrOnP
rivateNet
```

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.

Impact:

None - this is the default behavior.

Default Value:

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

References:

1. CCE-37959-4

CIS Controls:

Version 6

9 Limitation and Control of Network Ports, Protocols, and Services
Limitation and Control of Network Ports, Protocols, and Services

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

9.3 Perform Regular Automated Port Scans
Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.

18.5.10 Microsoft Peer-to-Peer Networking Services

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

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

18.5.10.1 (L2) Ensure 'Turn off Microsoft Peer-to-Peer Networking Services' is set to 'Enabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Peernet:Disabled
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Network\Microsoft
Peer-to-Peer Networking Services\Turn off Microsoft Peer-to-Peer Networking
Services
```

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

Impact:

Microsoft Peer-to-Peer Networking Services are turned off in their entirety, and all applications dependent on them will stop working.

Default Value:

Disabled. (Peer-to-peer protocols are turned on.)

References:

1. CCE-37699-6

CIS Controls:

Version 6

9.1 Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

9.3 Perform Regular Automated Port Scans
Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.

18.5.11 Network Connections

This section contains recommendations for Network Connections settings.

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

18.5.11.1 (L1) Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled' (Scored)

Profile Applicability:

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

Description:

You can use this procedure to controls user's ability to install and configure a Network Bridge.

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

Rationale:

The Network Bridge setting, if enabled, allows users to create a Layer 2 Media Access Control (MAC) bridge, enabling them to connect two or more physical network segments together. A Network Bridge thus allows a computer that has connections to two different networks to share data between those networks.

In an enterprise managed environment, where there is a need to control network traffic to only authorized paths, allowing users to create a Network Bridge increases the risk and attack surface from the bridged network.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Network
Connections:NC_AllowNetBridge_NLA
```

Remediation:

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

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

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

Impact:

Users cannot create or configure a Network Bridge.

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.)

References:

1. CCE-38002-2

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

4.3 Ensure the Use of Dedicated Administrative Accounts

Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.

18.5.11.2 (L1) Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

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

Remediation:

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

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

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `NetworkConnections.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Impact:

Domain users must elevate when setting a network's location.

Default Value:

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

References:

1. CCE-38188-9

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

4.3 Ensure the Use of Dedicated Administrative Accounts

Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.

18.5.12 Network Connectivity Status Indicator

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

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

18.5.13 Network Isolation

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

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

18.5.14 Network Provider

This section contains recommendations for Network Provider settings.

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

18.5.14.1 (L1) Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares' (Scored)

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" and "Require Integrity" set for all NETLOGON and SYSVOL shares.`

Note: If the environment exclusively contains Windows 8.0 / Server 2012 (non-R2) or newer systems, then the "`Privacy`" setting may (optionally) also be set to enable SMB encryption. However, using SMB encryption will render the targeted share paths completely inaccessible by older OSes, so only use this additional option with caution and thorough testing.

Rationale:

In February 2015, Microsoft released a new control mechanism to mitigate a security risk in Group Policy as part of the MS15-011 / MSKB 3000483 security update. This mechanism requires both the installation of the new security update and also the deployment of specific group policy settings to all computers on the domain from Windows Vista / Server 2008 (non-R2) or newer (the associated security patch to enable this feature was not released for Server 2003). A new group policy template (`NetworkProvider.admx/adml`) was also provided with the security update.

Once the new GPO template is in place, the following are the minimum requirements to remediate the Group Policy security risk:

```
\\*\NETLOGON RequireMutualAuthentication=1, RequireIntegrity=1
```

```
\\*\SYSVOL RequireMutualAuthentication=1, RequireIntegrity=1
```

Note: A reboot may be required after the setting is applied to a client machine to access the above paths.

Additional guidance on the deployment of this security setting is available from the Microsoft Premier Field Engineering (PFE) Platforms TechNet Blog here: Guidance on Deployment of MS15-011 and MS15-014.

Audit:

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

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\Harden
edPaths:\\*\NETLOGON
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\Harden
edPaths:\\*\SYSVOL
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled` with the following paths configured, at a minimum:

```
\\*\NETLOGON RequireMutualAuthentication=1, RequireIntegrity=1
\\*\SYSVOL RequireMutualAuthentication=1, RequireIntegrity=1
```

```
Computer Configuration\Policies\Administrative Templates\Network\Network
Provider\Hardened UNC Paths
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`NetworkProvider.admx/adml`) is required - it is included with the MS15-011 / MSKB 3000483 security update or with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

Impact:

Windows only allows access to the specified UNC paths after fulfilling additional security requirements.

Default Value:

Disabled. (No UNC paths are hardened.)

CIS Controls:

Version 6

3 Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

Version 7

3.1 Run Automated Vulnerability Scanning Tools

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.

18.5.15 Offline Files

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

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

18.5.16 QoS Packet Scheduler

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

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

18.5.17 SNMP

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

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

18.5.18 SSL Configuration Settings

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

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

18.5.19 TCPIP Settings

This section contains TCP/IP configuration settings.

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

18.5.19.1 IPv6 Transition Technologies

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

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

18.5.19.2 Parameters

This section contains TCP/IP parameter configuration settings.

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

18.5.19.2.1 (L2) Disable IPv6 (Ensure TCPIP6 Parameter 'DisabledComponents' is set to '0xff (255)') (Scored)

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.

Audit:

Navigate to the Registry path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration, set the following Registry value to `0xff (255) (DWORD)`:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TCPIP6\Parameters:Disabl
edComponents
```

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.

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.

Default Value:

All IPv6 components are enabled and Windows prefers IPv6 over IPv4.

CIS Controls:

Version 6

9 Limitation and Control of Network Ports, Protocols, and Services
Limitation and Control of Network Ports, Protocols, and Services

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

9.3 Perform Regular Automated Port Scans
Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.

18.5.20 Windows Connect Now

This section contains recommendations for Windows Connect Now settings.

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

18.5.20.1 (L2) Ensure 'Configuration of wireless settings using Windows Connect Now' is set to 'Disabled' (Scored)

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.

Audit:

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

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WCN\Registrars: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.

Impact:

WCN operations are disabled over all media.

Default Value:

WCN operations are enabled and allowed over all media.

References:

1. CCE-37481-9

CIS Controls:

Version 6

15.4 Configure Only Authorized Wireless Access On Client Machines

Where a specific business need for wireless access has been identified, configure wireless access on client machines to allow access only to authorized wireless networks. For devices that do not have an essential wireless business purpose, disable wireless access in the hardware configuration (basic input/output system or extensible firmware interface).

Version 7

15.4 Disable Wireless Access on Devices if Not Required

Disable wireless access on devices that do not have a business purpose for wireless access.

15.5 Limit Wireless Access on Client Devices

Configure wireless access on client machines that do have an essential wireless business purpose, to allow access only to authorized wireless networks and to restrict access to other wireless networks.

18.5.20.2 (L2) Ensure 'Prohibit access of the Windows Connect Now wizards' is set to 'Enabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WCN\UI:DisableWcnUi
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Network\Windows
Connect Now\Prohibit access of the Windows Connect Now wizards
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsConnectNow.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

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.

Default Value:

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

References:

1. CCE-36109-7

CIS Controls:

Version 6

15.4 Configure Only Authorized Wireless Access On Client Machines
Where a specific business need for wireless access has been identified, configure wireless access on client machines to allow access only to authorized wireless networks. For devices that do not have an essential wireless business purpose, disable wireless access in the hardware configuration (basic input/output system or extensible firmware interface).

Version 7

15.4 Disable Wireless Access on Devices if Not Required
Disable wireless access on devices that do not have a business purpose for wireless access.

15.5 Limit Wireless Access on Client Devices
Configure wireless access on client machines that do have an essential wireless business purpose, to allow access only to authorized wireless networks and to restrict access to other wireless networks.

18.5.21 Windows Connection Manager

This section contains recommendations for Windows Connection Manager settings.

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

18.5.21.1 (L1) Ensure 'Minimize the number of simultaneous connections to the Internet or a Windows Domain' is set to 'Enabled: 1 = Minimize simultaneous connections' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WcmSvc\GroupPolicy:fMi
nimizeConnections
```

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.

Impact:

None - this is the default behavior.

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.)

References:

1. CCE-38338-0

CIS Controls:

Version 6

12 Boundary Defense
Boundary Defense

Version 7

15.5 Limit Wireless Access on Client Devices
Configure wireless access on client machines that do have an essential wireless business purpose, to allow access only to authorized wireless networks and to restrict access to other wireless networks.

18.5.21.2 (L2) Ensure 'Prohibit connection to non-domain networks when connected to domain authenticated network' is set to 'Enabled' (MS only) (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WcmSvc\GroupPolicy:fBl
ockNonDomain
```

Remediation:

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

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

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WCM.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Impact:

The computer responds to automatic and manual network connection attempts based on the following circumstances:

Automatic connection attempts - When the computer is already connected to a domain based network, all automatic connection attempts to non-domain networks are blocked. - When the computer is already connected to a non-domain based network, automatic connection attempts to domain based networks are blocked.

Manual connection attempts - When the computer is already connected to either a non-domain based network or a domain based network over media other than Ethernet, and a user attempts to create a manual connection to an additional network in violation of this policy setting, the existing network connection is disconnected and the manual connection is allowed. - When the computer is already connected to either a non-domain based network or a domain based network over Ethernet, and a user attempts to create a manual connection to an additional network in violation of this policy setting, the existing Ethernet connection is maintained and the manual connection attempt is blocked.

Default Value:

Disabled. (Connections to both domain and non-domain networks are simultaneously allowed.)

References:

1. CCE-37627-7

CIS Controls:

Version 6

12 Boundary Defense
Boundary Defense

Version 7

12.2 Scan for Unauthorized Connections across Trusted Network Boundaries
Perform regular scans from outside each trusted network boundary to detect any unauthorized connections which are accessible across the boundary.

18.6 Printers

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

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

18.7 Start Menu and Taskbar

This section contains recommendations for Start Menu and Taskbar.

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

18.7.1 Notifications

This section contains recommendations for Start Menu and Taskbar Notifications.

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

18.7.1.1 (L2) Ensure 'Turn off notifications network usage' is set to 'Enabled' (Scored)

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 3rd-party notifications and updates from the cloud/Internet. In a high security environment, external systems, especially those hosted outside the organization, should be prevented from having an impact on the secure workstations.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\PushNot
ifications:NoCloudApplicationNotification
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Start Menu and
Taskbar\Turn off notifications network usage
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WPN.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Impact:

Applications and system features will not be able receive notifications from the network from WNS or via notification polling APIs.

Default Value:

Disabled.

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

9.3 Perform Regular Automated Port Scans
Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.

13.1 Maintain an Inventory Sensitive Information
Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located onsite or at a remote service provider.

18.8 System

This section contains recommendations for System settings.

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

18.8.1 Access-Denied Assistance

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

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

18.8.2 App-V

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

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

18.8.3 Audit Process Creation

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

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

18.8.3.1 (L1) Ensure 'Include command line in process creation events' is set to 'Disabled' (Scored)

Profile Applicability:

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

Description:

This policy setting determines what information is logged in security audit events when a new process has been created.

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

Rationale:

When this policy setting is enabled, any user who has read access to the security events can read the command-line arguments for any successfully created process. Command-line arguments may contain sensitive or private information such as passwords or user data.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

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

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\System\Audit Process
Creation\Include command line in process creation events
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `AuditSettings.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Impact:

None - this is the default behavior.

Default Value:

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

References:

1. CCE-36925-6

CIS Controls:

Version 6

16.14 Encrypt/Hash All Authentication Files And Monitor Their Access
Verify that all authentication files are encrypted or hashed and that these files cannot be accessed without root or administrator privileges. Audit all access to password files in the system.

Version 7

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

18.8.4 Credentials Delegation

This section contains settings related to Credential Delegation.

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

18.8.4.1 (L1) Ensure 'Encryption Oracle Remediation' is set to 'Enabled: Force Updated Clients' (Scored)

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).

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\
CredSSP\Parameters:AllowEncryptionOracle
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\System\Credentials
Delegation\Encryption Oracle Remediation
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `CredSsp.admx/adml` that is included with the Microsoft Windows 10 Release 1803 Administrative Templates (or newer).

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.

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:

Version 7

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

18.8.5 Device 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 `DeviceGuard.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

18.8.6 Device Health Attestation Service

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

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

18.8.7 Device Installation

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

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

18.8.8 Device Redirection

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

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

18.8.9 Disk NV Cache

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

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

18.8.10 Disk Quotas

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

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

18.8.11 Display

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

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

18.8.12 Distributed COM

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

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

18.8.13 Driver Installation

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

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

18.8.14 Early Launch Antimalware

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

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

18.8.14.1 (L1) Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good, unknown and bad but critical' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Policies\EarlyLaunch:DriverLoadPo
licy
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Good, unknown and bad but critical:`

```
Computer Configuration\Policies\Administrative Templates\System\Early Launch
Antimalware\Boot-Start Driver Initialization Policy
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `EarlyLaunchAM.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Impact:

None - this is the default behavior.

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.)

References:

1. CCE-37912-3

CIS Controls:

Version 6

8 Malware Defenses
Malware Defenses

Version 7

8.1 Utilize Centrally Managed Anti-malware Software
Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.

8.2 Ensure Anti-Malware Software and Signatures are Updated
Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.

18.8.15 Enhanced Storage Access

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

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

18.8.16 File Classification Infrastructure

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

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

18.8.17 File Share Shadow Copy Agent

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

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

18.8.18 File Share Shadow Copy Provider

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

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

18.8.19 Filesystem (formerly NTFS Filesystem)

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

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

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

18.8.20 Folder Redirection

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

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

18.8.21 Group Policy

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

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

18.8.21.1 (L1) Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE' (Scored)

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

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

Rationale:

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

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

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

Remediation:

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

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

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `GroupPolicy.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Impact:

Group Policies will be reapplied every time they are refreshed, which could have a slight impact on performance.

Default Value:

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

References:

1. CCE-36169-1

CIS Controls:

Version 6

3.7 Deploy System Configuration Management Tools (i.e. Remediation Tools)

Deploy system configuration management tools, such as Active Directory Group Policy Objects for Microsoft Windows systems or Puppet for UNIX systems that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals. They should be capable of triggering redeployment of configuration settings on a scheduled, manual, or event-driven basis.

Version 7

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.

5.5 Implement Automated Configuration Monitoring Systems

Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.

18.8.21.2 (L1) Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE' (Scored)

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 policies even if the policies have not changed.

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

Rationale:

Setting this option to true (checked) will ensure unauthorized changes that might have been configured locally are forced to match the domain-based Group Policy settings again.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

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

Remediation:

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

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

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `GroupPolicy.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Impact:

Group Policies will be reapplied even if they have not been changed, which could have a slight impact on performance.

Default Value:

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

References:

1. CCE-36169-1

CIS Controls:

Version 6

3.7 Deploy System Configuration Management Tools (i.e. Remediation Tools)
Deploy system configuration management tools, such as Active Directory Group Policy Objects for Microsoft Windows systems or Puppet for UNIX systems that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals. They should be capable of triggering redeployment of configuration settings on a scheduled, manual, or event-driven basis.

Version 7

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.

5.5 Implement Automated Configuration Monitoring Systems
Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.

18.8.21.3 (L1) Ensure 'Turn off background refresh of Group Policy' is set to 'Disabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is in effect when the following registry location does not exist:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:
DisableBkGndGroupPolicy
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\System\Group
Policy\Turn off background refresh of Group Policy
```

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

Impact:

None - this is the default behavior.

Default Value:

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

References:

1. CCE-37712-7

CIS Controls:

Version 6

3.7 Deploy System Configuration Management Tools (i.e. Remediation Tools)
Deploy system configuration management tools, such as Active Directory Group Policy Objects for Microsoft Windows systems or Puppet for UNIX systems that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals. They should be capable of triggering redeployment of configuration settings on a scheduled, manual, or event-driven basis.

Version 7

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.

5.5 Implement Automated Configuration Monitoring Systems
Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.

18.8.22 Internet Communication Management

This section contains recommendations related to Internet Communication Management.

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

18.8.22.1 Internet Communication settings

This section contains recommendations related to Internet Communication settings.

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

18.8.22.1.1 (L1) Ensure 'Turn off downloading of print drivers over HTTP' is set to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows
NT\Printers:DisableWebPnPDownload
```

Remediation:

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

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

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

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.

Default Value:

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

References:

1. CCE-36625-2

CIS Controls:

Version 6

2 Inventory of Authorized and Unauthorized Software
Inventory of Authorized and Unauthorized Software

Version 7

2.6 Address unapproved software
Ensure that unauthorized software is either removed or the inventory is updated in a timely manner

2.7 Utilize Application Whitelisting
Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.

18.8.22.1.2 (L2) Ensure 'Turn off handwriting personalization data sharing' is set to 'Enabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\TabletPC:PreventHandwr
itingDataSharing
```

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).

Impact:

Tablet PC users cannot choose to share writing samples from the handwriting recognition personalization tool with Microsoft.

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.

References:

1. CCE-37911-5

CIS Controls:

Version 6

13 Data Protection
Data Protection

Version 7

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

18.8.22.1.3 (L2) Ensure 'Turn off handwriting recognition error reporting' is set to 'Enabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\HandwritingErrorReport
s:PreventHandwritingErrorReports
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\System\Internet
Communication Management\Internet Communication settings\Turn off handwriting
recognition error reporting
```

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

Impact:

Users cannot start the handwriting recognition error reporting tool or send error reports to Microsoft.

Default Value:

Disabled. (Tablet PC users can report handwriting recognition errors to Microsoft.)

References:

1. CCE-36203-8

CIS Controls:

Version 6

13 Data Protection
Data Protection

Version 7

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

18.8.22.1.4 (L2) Ensure 'Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com' is set to 'Enabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Internet Connection
Wizard:ExitOnMSICW
```

Remediation:

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

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

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

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.

Default Value:

Disabled. (Users can connect to Microsoft to download a list of ISPs for their area.)

References:

1. CCE-37163-3

CIS Controls:

Version 6

13 Data Protection
Data Protection

Version 7

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

18.8.22.1.5 (L1) Ensure 'Turn off Internet download for Web publishing and online ordering wizards' is set to 'Enabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explore
r:NoWebServices
```

Remediation:

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

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

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

Impact:

Windows is prevented from downloading providers; only the service providers cached in the local registry are displayed.

Default Value:

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

References:

1. CCE-36096-6

CIS Controls:

Version 6

7 Email and Web Browser Protections
Email and Web Browser Protections

Version 7

7.4 Maintain and Enforce Network-Based URL Filters
Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.

18.8.22.1.6 (L2) Ensure 'Turn off printing over HTTP' is set to 'Enabled' (Scored)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows
NT\Printers:DisableHTTPPrinting
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\System\Internet
Communication Management\Internet Communication settings\Turn off printing
over HTTP
```

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

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.

Default Value:

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

References:

1. CCE-36920-7

CIS Controls:

Version 6

13.1 Assess Data To Identify Sensitive Information
Perform an assessment of data to identify sensitive information that requires the application of encryption and integrity controls.

Version 7

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

18.8.22.1.7 (L2) Ensure 'Turn off Registration if URL connection is referring to Microsoft.com' is set to 'Enabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Registration Wizard
Control:NoRegistration
```

Remediation:

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

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

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

Impact:

Users are blocked from connecting to Microsoft.com for online registration and they cannot register their copy of Windows online.

Default Value:

Disabled. (Users can connect to Microsoft.com to complete the online Windows Registration.)

References:

1. CCE-36352-3

CIS Controls:

Version 7

7.4 Maintain and Enforce Network-Based URL Filters

Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.

18.8.22.1.8 (L2) Ensure 'Turn off Search Companion content file updates' is set to 'Enabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\SearchCompanion:DisableContent
FileUpdates
```

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.

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.

Default Value:

Disabled. (Search Companion downloads content updates unless the user is using Classic Search.)

References:

1. CCE-36884-5

CIS Controls:

Version 6

13 Data Protection
Data Protection

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

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

18.8.22.1.9 (L2) Ensure 'Turn off the "Order Prints" picture task' is set to 'Enabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explore
r:NoOnlinePrintsWizard
```

Remediation:

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

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

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

Impact:

The task "Order Prints Online" is removed from Picture Tasks in File Explorer folders.

Default Value:

Disabled. (The "Order Prints Online" task is displayed in Picture Tasks in File Explorer folders.)

References:

1. CCE-38275-4

CIS Controls:

Version 6

13 Data Protection
Data Protection

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

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

18.8.22.1.10 (L2) Ensure 'Turn off the "Publish to Web" task for files and folders' is set to 'Enabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explore
r:NoPublishingWizard
```

Remediation:

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

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

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

Impact:

The "Publish to Web" task is removed from File and Folder tasks in Windows folders.

Default Value:

Disabled. (The "Publish to Web" task is shown in File and Folder tasks in Windows folders.)

References:

1. CCE-37090-8

CIS Controls:

Version 6

13 Data Protection
Data Protection

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

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

18.8.22.1.11 (L2) Ensure 'Turn off the Windows Messenger Customer Experience Improvement Program' is set to 'Enabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Messenger\Client:CEIP
```

Remediation:

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

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

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

Impact:

Windows Messenger will not collect usage information, and the user settings to enable the collection of usage information will not be shown.

Default Value:

Users have the choice to opt-in and allow information to be collected.

References:

1. CCE-36628-6

CIS Controls:

Version 6

13 Data Protection
Data Protection

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

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

18.8.22.1.12 (L2) Ensure 'Turn off Windows Customer Experience Improvement Program' is set to 'Enabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\SQMClient\Windows:CEIPEnable
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\System\Internet
Communication Management\Internet Communication settings\Turn off Windows
Customer Experience Improvement Program
```

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

Impact:

All users are opted out of the Windows Customer Experience Improvement Program.

Default Value:

The Administrator can use the Problem Reports and Solutions component in Control Panel to enable Windows Customer Experience Improvement Program for all users.

References:

1. CCE-36174-1

CIS Controls:

Version 6

13 Data Protection
Data Protection

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

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

18.8.22.1.13 (L2) Ensure 'Turn off Windows Error Reporting' is set to 'Enabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows Error
Reporting:Disabled
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\PCHealth\ErrorReporting:DoRepo
rt
```

Remediation:

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

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

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

Impact:

Users are not given the option to report errors to Microsoft.

Default Value:

Disabled. (Errors may be reported to Microsoft via the Internet or to a corporate file share.)

References:

1. CCE-35964-6

CIS Controls:

Version 6

13 Data Protection
Data Protection

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

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

18.8.23 iSCSI

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

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

18.8.24 KDC

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

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

18.8.25 Kerberos

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

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

18.8.26 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).

18.8.27 Locale Services

This section contains recommendations for Locale Services settings.

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

18.8.27.1 (L2) Ensure 'Disallow copying of user input methods to the system account for sign-in' is set to 'Enabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Control
Panel\International:BlockUserInputMethodsForSignIn
```

Remediation:

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

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

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Globalization.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Impact:

Users will have input methods enabled for the system account on the sign-in page.

Default Value:

Disabled. (Users will be able to use input methods enabled for their user account on the sign-in page.)

References:

1. CCE-36343-2

CIS Controls:

Version 6

16.5 Ensure Workstation Screen Locks Are Configured
Configure screen locks on systems to limit access to unattended workstations.

Version 7

16.11 Lock Workstation Sessions After Inactivity
Automatically lock workstation sessions after a standard period of inactivity.

18.8.28 Logon

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

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

18.8.28.1 (L1) Ensure 'Do not display network selection UI' is set to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System:DontDisplayNetw
orkSelectionUI
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\System\Logon\Do not
display network selection UI
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Logon.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Impact:

The PC's network connectivity state cannot be changed without signing into Windows.

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.)

References:

1. CCE-38353-9

CIS Controls:

Version 6

5 Controlled Use of Administration Privileges
Controlled Use of Administration Privileges

Version 7

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.

18.8.28.2 (L1) Ensure 'Do not enumerate connected users on domain-joined computers' is set to 'Enabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System:DontEnumerateCo
nnectedUsers
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\System\Logon\Do not
enumerate connected users on domain-joined computers
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Logon.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Impact:

The Logon UI will not enumerate any connected users on domain-joined computers.

Default Value:

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

References:

1. CCE-37838-0

CIS Controls:

Version 6

16.9 Configure Account Access Centrally

Configure access for all accounts through a centralized point of authentication, for example Active Directory or LDAP. Configure network and security devices for centralized authentication as well.

Version 7

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.

18.8.28.3 (L1) Ensure 'Enumerate local users on domain-joined computers' is set to 'Disabled' (MS only) (Scored)

Profile Applicability:

- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System:EnumerateLocalU
sers
```

Remediation:

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

```
Computer Configuration\Policies\Administrative
Templates\System\Logon\Enumerate local users on domain-joined computers
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Logon.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Impact:

None - this is the default behavior.

Default Value:

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

References:

1. CCE-35894-5

CIS Controls:

Version 6

16.9 Configure Account Access Centrally
Configure access for all accounts through a centralized point of authentication, for example Active Directory or LDAP. Configure network and security devices for centralized authentication as well.

Version 7

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.

18.8.28.4 (L1) Ensure 'Turn off app notifications on the lock screen' is set to 'Enabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System:DisableLockScre
enAppNotifications
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\System\Logon\Turn
off app notifications on the lock screen
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Logon.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Impact:

No app notifications are displayed on the lock screen.

Default Value:

Disabled. (Users can choose which apps display notifications on the lock screen.)

References:

1. CCE-35893-7

CIS Controls:

Version 6

16.5 Ensure Workstation Screen Locks Are Configured
Configure screen locks on systems to limit access to unattended workstations.

Version 7

16.11 Lock Workstation Sessions After Inactivity
Automatically lock workstation sessions after a standard period of inactivity.

18.8.28.5 (L1) Ensure 'Turn off picture password sign-in' is set to 'Enabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System:BlockDomainPict
urePassword
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\System\Logon\Turn
off picture password sign-in
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `CredentialProviders.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Impact:

Users will not be able to set up or sign in with a picture password.

Default Value:

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

References:

1. CCE-37830-7

CIS Controls:

Version 6

16.5 Ensure Workstation Screen Locks Are Configured
Configure screen locks on systems to limit access to unattended workstations.

Version 7

16.11 Lock Workstation Sessions After Inactivity
Automatically lock workstation sessions after a standard period of inactivity.

18.8.28.6 (L1) Ensure 'Turn on convenience PIN sign-in' is set to 'Disabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System:AllowDomainPINL
ogon
```

Remediation:

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

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

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `CredentialProviders.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).
Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Turn on PIN sign-in*, but it was renamed starting with the Windows 10 Release 1511 Administrative Templates.

Impact:

None - this is the default behavior.

Default Value:

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

References:

1. CCE-37528-7

CIS Controls:

Version 6

16.5 Ensure Workstation Screen Locks Are Configured
Configure screen locks on systems to limit access to unattended workstations.

Version 7

16.11 Lock Workstation Sessions After Inactivity
Automatically lock workstation sessions after a standard period of inactivity.

18.8.29 Mitigation Options

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

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

18.8.30 Net Logon

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

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

18.8.31 OS Policies

This section is 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).

18.8.32 Performance Control Panel

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

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

18.8.33 PIN Complexity

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

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

18.8.34 Power Management

This section contains recommendations for Power Management settings.

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

18.8.34.1 Button Settings

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

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

18.8.34.2 Energy Saver Settings

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

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

18.8.34.3 Hard Disk Settings

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

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

18.8.34.4 Notification Settings

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

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

18.8.34.5 Power Throttling Settings

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

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

18.8.34.6 Sleep Settings

This section contains recommendations related to Power Management Sleep mode.

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

18.8.34.6.1 (L1) Ensure 'Require a password when a computer wakes (on battery)' is set to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

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

Remediation:

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

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

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Power.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Impact:

None - this is the default behavior.

Default Value:

Enabled. (The user is prompted for a password when the system resumes from sleep while on battery.)

References:

1. CCE-36881-1

CIS Controls:

Version 6

16.5 Ensure Workstation Screen Locks Are Configured
Configure screen locks on systems to limit access to unattended workstations.

Version 7

16.11 Lock Workstation Sessions After Inactivity
Automatically lock workstation sessions after a standard period of inactivity.

18.8.34.6.2 (L1) Ensure 'Require a password when a computer wakes (plugged in)' is set to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

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

Remediation:

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

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

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Power.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Impact:

None - this is the default behavior.

Default Value:

Enabled. (The user is prompted for a password when the system resumes from sleep while plugged in.)

References:

1. CCE-37066-8

CIS Controls:

Version 6

16.5 Ensure Workstation Screen Locks Are Configured
Configure screen locks on systems to limit access to unattended workstations.

Version 7

16.11 Lock Workstation Sessions After Inactivity
Automatically lock workstation sessions after a standard period of inactivity.

18.8.35 Recovery

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

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

18.8.36 Remote Assistance

This section contains recommendations related to Remote Assistance.

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

18.8.36.1 (L1) Ensure 'Configure Offer Remote Assistance' is set to 'Disabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

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

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\System\Remote
Assistance\Configure Offer Remote Assistance
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `RemoteAssistance.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Impact:

None - this is the default behavior.

Default Value:

Disabled. (Users on this computer cannot get help from their corporate technical support staff using Offer (Unsolicited) Remote Assistance.)

References:

1. CCE-36388-7

CIS Controls:

Version 6

9.1 Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

18.8.36.2 (L1) Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services:fAllowToGetHelp
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\System\Remote
Assistance\Configure Solicited Remote Assistance
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `RemoteAssistance.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

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.

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.

References:

1. CCE-37281-3

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

18.8.37 Remote Procedure Call

This section contains recommendations related to Remote Procedure Call.

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

18.8.37.1 (L1) Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled' (MS only) (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows
NT\Rpc:EnableAuthEpResolution
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\System\Remote
Procedure Call\Enable RPC Endpoint Mapper Client Authentication
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `RPC.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

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.

Default Value:

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

References:

1. CCE-37346-4

CIS Controls:

Version 6

9.1 Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

18.8.37.2 (L2) Ensure 'Restrict Unauthenticated RPC clients' is set to 'Enabled: Authenticated' (MS only) (Scored)

Profile Applicability:

- Level 2 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows
NT\Rpc:RestrictRemoteClients
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\System\Remote
Procedure Call\Restrict Unauthenticated RPC clients
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `RPC.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

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.

Default Value:

Enabled: None. (All RPC clients are allowed to connect to RPC servers running on the machine.)

References:

1. CCE-36559-3

CIS Controls:

Version 6

9.1 Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

18.8.38 Removable Storage Access

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

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

18.8.39 Scripts

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

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

18.8.40 Server Manager

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

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

18.8.41 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).

18.8.42 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).

18.8.43 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.

18.8.44 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).

18.8.45 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).

18.8.46 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.

18.8.47 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.

18.8.47.1 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.

18.8.47.2 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.

18.8.47.3 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.

18.8.47.4 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).

18.8.47.5 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.

18.8.47.5.1 (L2) Ensure 'Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider' is set to 'Disabled' (Scored)

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 3rd party since this data could contain sensitive information.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\ScriptedDiagnosticsPro
vider\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).

Impact:

MSDT cannot run in support mode, and no data can be collected or sent to the support provider.

Default Value:

Enabled. (Users can use MSDT to collect and send diagnostic data to a support professional to resolve a problem. By default, the support provider is set to Microsoft Corporation.)

References:

1. CCE-38161-6

CIS Controls:

Version 6

13 Data Protection
Data Protection

Version 7

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

18.8.47.6 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).

18.8.47.7 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).

18.8.47.8 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).

18.8.47.9 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.

18.8.47.10 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.

18.8.47.11 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).

18.8.47.11.1 (L2) Ensure 'Enable/Disable PerfTrack' is set to 'Disabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WDI\{9c5a40da-b965-4fc3-8781-88dd50a6299d}:ScenarioExecutionEnabled
```

Remediation:

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

```
Computer Configuration\Policies\Administrative
Templates\System\Troubleshooting and Diagnostics\Windows Performance
PerfTrack\Enable/Disable PerfTrack
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `PerformancePerftrack.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Impact:

Responsiveness events are not processed.

Default Value:

Enabled. (Responsiveness events are processed and aggregated. The aggregated data will be transmitted to Microsoft through SQM.)

References:

1. CCE-36648-4

CIS Controls:

Version 6

13 Data Protection
Data Protection

Version 7

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

18.8.48 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.

18.8.49 User 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 `UserProfiles.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.50 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.

18.8.51 Windows HotStart

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

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

18.8.52 Windows Time Service

This section contains recommendations related to the Windows Time Service.

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

18.8.52.1 Time Providers

This section contains recommendations related to Time Providers.

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

18.8.52.1.1 (L2) Ensure 'Enable Windows NTP Client' is set to 'Enabled' (Scored)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - 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 state for this setting is: `Enabled`.

Rationale:

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

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\W32Time\TimeProviders\NtpClien
t: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.

Impact:

You can set the local computer clock to synchronize time with NTP servers.

Default Value:

Disabled. (The local computer clock does not synchronize time with NTP servers.)

References:

1. CCE-37843-0

CIS Controls:

Version 6

6.1 Use At Least Two Synchronized Time Sources For All Servers And Network Equipment

Include at least two synchronized time sources from which all servers and network equipment retrieve time information on a regular basis so that timestamps in logs are consistent.

Version 7

6.1 Utilize Three Synchronized Time Sources

Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.

18.8.52.1.2 (L2) Ensure 'Enable Windows NTP Server' is set to 'Disabled' (MS only) (Scored)

Profile Applicability:

- Level 2 - Member Server

Description:

This policy setting allows you to specify whether the Windows NTP Server is enabled.

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\W32Time\TimeProviders\NtpServe
r: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.

Impact:

None - this is the default behavior.

Default Value:

Disabled. (The computer cannot service NTP requests from other computers.)

References:

1. CCE-37319-1

CIS Controls:

Version 6

9.1 Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

18.9 Windows Components

This section contains recommendations for Windows Component settings.

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

18.9.1 Active Directory Federation Services

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

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

18.9.2 ActiveX Installer Service

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

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

18.9.3 Add features to Windows 8 / 8.1 / 10 (formerly Windows Anytime Upgrade)

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

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

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

18.9.4 App Package Deployment

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

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

18.9.5 App Privacy

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

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

18.9.6 App runtime

This section is 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).

18.9.7 Application Compatibility

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

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

18.9.8 AutoPlay Policies

This section contains recommendations for AutoPlay policies.

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

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Explorer:NoAutoplayfor
nonVolume
```

Remediation:

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

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

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `AutoPlay.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Impact:

AutoPlay will not be allowed for MTP devices like cameras or phones.

Default Value:

Disabled. (AutoPlay is enabled for non-volume devices.)

References:

1. CCE-37636-8

CIS Controls:

Version 6

8.3 Limit Use Of External Devices (i.e. USB)
Limit use of external devices to those with an approved, documented business need. Monitor for use and attempted use of external devices. Configure laptops, workstations, and servers so that they will not auto-run content from removable media, like USB tokens (i.e., "thumb drives"), USB hard drives, CDs/DVDs, FireWire devices, external serial advanced technology attachment devices, and mounted network shares. Configure systems so that they automatically conduct an anti-malware scan of removable media when inserted.

Version 7

8.4 Configure Anti-Malware Scanning of Removable Devices
Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.

8.5 Configure Devices Not To Auto-run Content
Configure devices to not auto-run content from removable media.

18.9.8.2 (L1) Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explore
r:NoAutorun
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`: `Do not execute any autorun commands`:

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

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `AutoPlay.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Impact:

AutoRun commands will be completely disabled.

Default Value:

Disabled. (Windows will prompt the user whether autorun command is to be run.)

References:

1. CCE-38217-6

CIS Controls:

Version 6

8.3 Limit Use Of External Devices (i.e. USB)
Limit use of external devices to those with an approved, documented business need. Monitor for use and attempted use of external devices. Configure laptops, workstations, and servers so that they will not auto-run content from removable media, like USB tokens (i.e., "thumb drives"), USB hard drives, CDs/DVDs, FireWire devices, external serial advanced technology attachment devices, and mounted network shares. Configure systems so that they automatically conduct an anti-malware scan of removable media when inserted.

Version 7

8.4 Configure Anti-Malware Scanning of Removable Devices
Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.

8.5 Configure Devices Not To Auto-run Content
Configure devices to not auto-run content from removable media.

18.9.8.3 (L1) Ensure 'Turn off Autoplay' is set to 'Enabled: All drives' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explore
r: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.

Impact:

Autoplay will be disabled - users will have to manually launch setup or installation programs that are provided on removable media.

Default Value:

Disabled. (Autoplay is enabled.)

References:

1. CCE-36875-3

CIS Controls:

Version 6

8.3 Limit Use Of External Devices (i.e. USB)

Limit use of external devices to those with an approved, documented business need. Monitor for use and attempted use of external devices. Configure laptops, workstations, and servers so that they will not auto-run content from removable media, like USB tokens (i.e., "thumb drives"), USB hard drives, CDs/DVDs, FireWire devices, external serial advanced technology attachment devices, and mounted network shares. Configure systems so that they automatically conduct an anti-malware scan of removable media when inserted.

Version 7

8.4 Configure Anti-Malware Scanning of Removable Devices

Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.

8.5 Configure Devices Not To Auto-run Content

Configure devices to not auto-run content from removable media.

18.9.9 Backup

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

This Group Policy section is provided by the Group Policy template `UserDataBackup.admx/adml` that is only included with the Microsoft Windows Vista through the Windows 10 Release 1511 Administrative Templates (except for the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates).

18.9.10 Biometrics

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

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

18.9.11 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.

18.9.12 Camera

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

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

18.9.13 Cloud Content

This section is 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).

18.9.14 Connect

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

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

18.9.15 Credential User Interface

This section contains recommendations related to the Credential User Interface.

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

18.9.15.1 (L1) Ensure 'Do not display the password reveal button' is set to 'Enabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CredUI:DisablePassword
Reveal
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Credential User Interface\Do not display the password reveal
button
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `CredUI.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Impact:

The password reveal button will not be displayed after a user types a password in the password entry text box.

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.)

References:

1. CCE-37534-5

CIS Controls:

Version 6

16 Account Monitoring and Control
Account Monitoring and Control

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

18.9.15.2 (L1) Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\CredUI:
EnumerateAdministrators
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Credential User Interface\Enumerate administrator accounts on
elevation
```

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

Impact:

None - this is the default behavior.

Default Value:

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

References:

1. CCE-36512-2

CIS Controls:

Version 6

16 Account Monitoring and Control
Account Monitoring and Control

Version 7

4.5 Use Multifactor Authentication For All Administrative Access
Use multi-factor authentication and encrypted channels for all administrative account access.

18.9.16 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 `Windows.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

18.9.17 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).

18.9.18 Desktop Gadgets

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

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

18.9.19 Desktop Window Manager

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

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

18.9.20 Device and Driver Compatibility

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

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

18.9.21 Device Registration (formerly Workplace Join)

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

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

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

18.9.22 Digital Locker

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

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

18.9.23 Edge UI

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

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

18.9.24 EMET

This section contains recommendations for configuring Microsoft Enhanced Mitigation Experience Toolkit (EMET).

This Group Policy section is provided by the Group Policy template `EMET.admx/adml` that is included with Microsoft EMET.

EMET is free and supported security software developed by Microsoft that allows an enterprise to apply exploit mitigations to applications that run on Windows. Many of these mitigations were later coded directly into Windows 10 and Server 2016.

Note: Although EMET is quite effective at enhancing exploit protection on Windows server OSes prior to Server 2016, it is highly recommended that compatibility testing is done on typical server configurations (including all CIS-recommended EMET settings) before widespread deployment to your environment.

Note #2: EMET has been reported to be very problematic on 32-bit OSes - we only recommend using it with 64-bit OSes.

Note #3: Microsoft has announced that EMET will be End-Of-Life (EOL) on July 31, 2018. This does not mean the software will stop working, only that Microsoft will not update it any further past that date, nor troubleshoot new problems with it. They are instead recommending that servers be upgraded to Server 2016.

18.9.24.1 (L1) Ensure 'EMET 5.52' or higher is installed (Scored)

Profile Applicability:

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

Description:

The Enhanced Mitigation Experience Toolkit (EMET) is free and supported security software developed by Microsoft that allows an enterprise to apply exploit mitigations to applications that run on Windows. Many of these mitigations were later coded directly into Windows 10 and Server 2016.

More information on EMET, including download and User Guide, can be obtained here:

Enhanced Mitigation Experience Toolkit - EMET - TechNet Security

Note: Although EMET is quite effective at enhancing exploit protection on Windows server OSes prior to Server 2016, it is highly recommended that compatibility testing is done on typical server configurations (including all CIS-recommended EMET settings) before widespread deployment to your environment.

Note #2: Microsoft has announced that EMET will be End-Of-Life (EOL) on July 31, 2018. This does not mean the software will stop working, only that Microsoft will not update it any further past that date, nor troubleshoot new problems with it. They are instead recommending that servers be upgraded to Server 2016.

Note #3: EMET has been reported to be very problematic on 32-bit OSes - we only recommend using it with 64-bit OSes.

Rationale:

EMET mitigations help reduce the reliability of exploits that target vulnerable software running on Windows.

Audit:

Navigate to `Control Panel\Program\Programs and Features` and confirm "EMET 5.52" or higher is listed in the `Name` column.

Remediation:

Install EMET 5.52 or higher.

CIS Controls:

Version 6

8.4 Enable Anti-exploitation Features (i.e. DEP, ASLR, EMET)

Enable anti-exploitation features such as Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualization/containerization, etc. For increased protection, deploy capabilities such as Enhanced Mitigation Experience Toolkit (EMET) that can be configured to apply these protections to a broader set of applications and executables.

Version 7

8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies

Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.

18.9.24.2 (L1) Ensure 'Default Action and Mitigation Settings' is set to 'Enabled' (plus subsettings) (Scored)

Profile Applicability:

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

Description:

This setting configures the default action after detection and advanced ROP mitigation.

The recommended state for this setting is:

- Default Action and Mitigation Settings - `Enabled`
- Deep Hooks - `Enabled`
- Anti Detours - `Enabled`
- Banned Functions - `Enabled`
- Exploit Action -`User Configured`

Rationale:

These advanced mitigations for ROP mitigations apply to all configured software in EMET:

- **Deep Hooks** protects critical APIs and the subsequent lower level APIs used by the top level critical API.
- **Anti Detours** renders ineffective exploits that evade hooks by executing a copy of the hooked function prologue and then jump to the function past the prologue.
- **Banned Functions** will block calls to `ntdll!LdrHotPatchRoutine` to mitigate potential exploits abusing the API.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\EMET\SysSettings:AntiDetours
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\EMET\SysSettings:BannedFunctio
ns
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\EMET\SysSettings:DeepHooks
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\EMET\SysSettings:ExploitAction
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\EMET\Default Action and Mitigation Settings
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`EMET.admx/adml`) is required - it is included with Microsoft Enhanced Mitigation Experience Toolkit (EMET).

Impact:

The advanced mitigations available in EMET will be enabled and actively applied to all software they are configured for.

Default Value:

User configured.

References:

1. CCE-38427-1

CIS Controls:

Version 6

8.4 Enable Anti-exploitation Features (i.e. DEP, ASLR, EMET)

Enable anti-exploitation features such as Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualization/containerization, etc. For increased protection, deploy capabilities such as Enhanced Mitigation Experience Toolkit (EMET) that can be configured to apply these protections to a broader set of applications and executables.

Version 7

8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies

Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.

18.9.24.3 (L1) Ensure 'Default Protections for Internet Explorer' is set to 'Enabled' (Scored)

Profile Applicability:

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

Description:

This setting determines if recommended EMET mitigations are applied to Internet Explorer.

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

Rationale:

Applying EMET mitigations to Internet Explorer will help reduce the reliability of exploits that target it.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\EMET\Defaults\IE
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\EMET\Default Protections for Internet Explorer
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`EMET.admx/adml`) is required - it is included with Microsoft Enhanced Mitigation Experience Toolkit (EMET).

Impact:

EMET mitigations will be applied to Internet Explorer.

Default Value:

User configured.

References:

1. CCE-38428-9

CIS Controls:

Version 6

8.4 Enable Anti-exploitation Features (i.e. DEP, ASLR, EMET)

Enable anti-exploitation features such as Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualization/containerization, etc. For increased protection, deploy capabilities such as Enhanced Mitigation Experience Toolkit (EMET) that can be configured to apply these protections to a broader set of applications and executables.

Version 7

8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies

Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.

18.9.24.4 (L1) Ensure 'Default Protections for Popular Software' is set to 'Enabled' (Scored)

Profile Applicability:

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

Description:

This setting determines if recommended EMET mitigations are applied to the following popular software:

- 7-Zip
- Adobe Photoshop
- Foxit Reader
- Google Chrome
- Google Talk
- iTunes
- Microsoft Live Writer
- Microsoft Lync Communicator
- Microsoft Photo Gallery
- Microsoft SkyDrive
- mIRC
- Mozilla Firefox
- Mozilla Thunderbird
- Opera
- Pidgin
- QuickTime Player
- RealPlayer
- Safari
- Skype
- VideoLAN VLC
- Winamp
- Windows Live Mail
- Windows Media Player
- WinRAR
- WinZip

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

Rationale:

Applying EMET mitigations to popular software packages will help reduce the reliability of exploits that target 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 many registry values (for the various popular software that EMET supports) under the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\EMET\Defaults
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\EMET\Default Protections for Popular Software
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`EMET.admx/adml`) is required - it is included with Microsoft Enhanced Mitigation Experience Toolkit (EMET).

Impact:

EMET mitigations will be applied to the listed popular software that is installed on the computer.

Default Value:

User configured.

References:

1. CCE-36750-8

CIS Controls:

Version 6

8.4 Enable Anti-exploitation Features (i.e. DEP, ASLR, EMET)

Enable anti-exploitation features such as Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualization/containerization, etc. For increased protection, deploy capabilities such as Enhanced Mitigation Experience Toolkit (EMET) that can be configured to apply these protections to a broader set of applications and executables.

Version 7

8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies

Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.

18.9.24.5 (L1) Ensure 'Default Protections for Recommended Software' is set to 'Enabled' (Scored)

Profile Applicability:

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

Description:

This setting determines if recommended EMET mitigations are applied to the following software:

- Adobe Acrobat
- Adobe Acrobat Reader
- Microsoft Office suite applications
- Oracle Java
- WordPad

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

Rationale:

Applying EMET mitigations to recommended software will help reduce the reliability of exploits that target 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 many registry values (for the various recommended software that EMET supports) under the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\EMET\Defaults
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\EMET\Default Protections for Recommended Software
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`EMET.admx/adml`) is required - it is included with Microsoft Enhanced Mitigation Experience Toolkit (EMET).

Impact:

EMET mitigations will be applied to the listed recommended software that is installed on the computer.

Default Value:

User configured.

References:

1. CCE-36515-5

CIS Controls:

Version 6

8.4 Enable Anti-exploitation Features (i.e. DEP, ASLR, EMET)

Enable anti-exploitation features such as Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualization/containerization, etc. For increased protection, deploy capabilities such as Enhanced Mitigation Experience Toolkit (EMET) that can be configured to apply these protections to a broader set of applications and executables.

Version 7

8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies

Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.

18.9.24.6 (L1) Ensure 'System ASLR' is set to 'Enabled: Application Opt-In' (Scored)

Profile Applicability:

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

Description:

This setting determines how applications become enrolled in Address Space Layout Randomization (ASLR).

The recommended state for this setting is: `Enabled: Application Opt-In`.

Rationale:

ASLR reduces the predictability of process memory, which in-turn helps reduce the reliability of exploits targeting memory corruption vulnerabilities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\EMET\SysSettings:ASLR
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\EMET\System ASLR
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`EMET.admx/adml`) is required - it is included with Microsoft Enhanced Mitigation Experience Toolkit (EMET).

Impact:

ASLR protections will be enabled on applications that have been configured for it in EMET.

Default Value:

User configured.

References:

1. CCE-38437-0

CIS Controls:

Version 6

8.4 Enable Anti-exploitation Features (i.e. DEP, ASLR, EMET)

Enable anti-exploitation features such as Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualization/containerization, etc. For increased protection, deploy capabilities such as Enhanced Mitigation Experience Toolkit (EMET) that can be configured to apply these protections to a broader set of applications and executables.

Version 7

8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies

Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.

18.9.24.7 (L1) Ensure 'System DEP' is set to 'Enabled: Application Opt-Out' (Scored)

Profile Applicability:

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

Description:

This setting determines how applications become enrolled in Data Execution Protection (DEP).

The recommended state for this setting is: `Enabled: Application Opt-Out`.

Rationale:

DEP marks pages of application memory as non-executable, which reduces a given exploit's ability to run attacker-controlled code.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\EMET\SysSettings:DEP
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\EMET\System DEP
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`EMET.admx/adml`) is required - it is included with Microsoft Enhanced Mitigation Experience Toolkit (EMET).

Impact:

DEP protections will be enabled on *all* applications unless EMET has been specifically configured to opt-out of DEP for that application.

Default Value:

User configured.

References:

1. CCE-38438-8

CIS Controls:

Version 6

8.4 Enable Anti-exploitation Features (i.e. DEP, ASLR, EMET)

Enable anti-exploitation features such as Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualization/containerization, etc. For increased protection, deploy capabilities such as Enhanced Mitigation Experience Toolkit (EMET) that can be configured to apply these protections to a broader set of applications and executables.

Version 7

8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies

Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.

18.9.24.8 (L1) Ensure 'System SEHOP' is set to 'Enabled: Application Opt-Out' (Scored)

Profile Applicability:

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

Description:

This setting determines how applications become enrolled in Structured Exception Handler Overwrite Protection (SEHOP).

The recommended state for this setting is: `Enabled: Application Opt-Out`.

Rationale:

When a software component suffers from a memory corruption vulnerability, an exploit may be able to overwrite memory that contains data structures that control how the software handles exceptions. By corrupting these structures in a controlled manner, an exploit may be able to execute arbitrary code. SEHOP verifies the integrity of those structures before they are used to handle exceptions, which reduces the reliability of exploits that leverage structured exception handler overwrites.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\EMET\SysSettings:SEHOP
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\EMET\System SEHOP
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`EMET.admx/adml`) is required - it is included with Microsoft Enhanced Mitigation Experience Toolkit (EMET).

Impact:

SEHOP protections will be enabled on *all* applications unless EMET has been specifically configured to opt-out of SEHOP for that application.

Default Value:

User configured.

References:

1. CCE-38439-6

CIS Controls:

Version 6

8.4 Enable Anti-exploitation Features (i.e. DEP, ASLR, EMET)
Enable anti-exploitation features such as Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualization/containerization, etc. For increased protection, deploy capabilities such as Enhanced Mitigation Experience Toolkit (EMET) that can be configured to apply these protections to a broader set of applications and executables.

Version 7

8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies
Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.

18.9.25 Event Forwarding

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

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

18.9.26 Event Log Service

This section contains recommendations for configuring the Event Log Service.

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

18.9.26.1 Application

This section contains recommendations for configuring the Application Event Log.

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

18.9.26.1.1 (L1) Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\EventLog\Application:R
etention
```

Remediation:

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

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

Note: This Group Policy path is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.
Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Retain old events*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Impact:

None - this is the default behavior.

Default Value:

Disabled. (When a log file reaches its maximum size, new events overwrite old events.)

References:

1. CCE-37775-4

CIS Controls:

Version 6

6.3 Ensure Audit Logging Systems Are Not Subject To Loss (i.e. rotation/archive)
Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals. The logs must be archived and digitally signed on a periodic basis.

Version 7

6.4 Ensure adequate storage for logs
Ensure that all systems that store logs have adequate storage space for the logs generated.

18.9.26.1.2 (L1) Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\EventLog\Application:M
axSize
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 32,768 or greater`:

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

Note: This Group Policy path is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.
Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Maximum Log Size (KB)*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Impact:

When event logs fill to capacity, they will stop recording information unless the retention method for each is set so that the computer will overwrite the oldest entries with the most recent ones. To mitigate the risk of loss of recent data, you can configure the retention method so that older events are overwritten as needed.

The consequence of this configuration is that older events will be removed from the logs. Attackers can take advantage of such a configuration, because they can generate a large number of extraneous events to overwrite any evidence of their attack. These risks can be somewhat reduced if you automate the archival and backup of event log data.

Ideally, all specifically monitored events should be sent to a server that uses Microsoft System Center Operations Manager (SCOM) or some other automated monitoring tool. Such a configuration is particularly important because an attacker who successfully compromises a server could clear the Security log. If all events are sent to a monitoring server, then you will be able to gather forensic information about the attacker's activities.

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.)

References:

1. CCE-37948-7

CIS Controls:

Version 6

6.3 Ensure Audit Logging Systems Are Not Subject To Loss (i.e. rotation/archive)
Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals. The logs must be archived and digitally signed on a periodic basis.

Version 7

6.4 Ensure adequate storage for logs
Ensure that all systems that store logs have adequate storage space for the logs generated.

18.9.26.2 Security

This section contains recommendations for configuring the Security Event Log.

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

18.9.26.2.1 (L1) Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\EventLog\Security:Rete
ntion
```

Remediation:

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

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

Note: This Group Policy path is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.
Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Retain old events*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Impact:

None - this is the default behavior.

Default Value:

Disabled. (When a log file reaches its maximum size, new events overwrite old events.)

References:

1. CCE-37145-0

CIS Controls:

Version 6

6.3 Ensure Audit Logging Systems Are Not Subject To Loss (i.e. rotation/archive)
Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals. The logs must be archived and digitally signed on a periodic basis.

Version 7

6.4 Ensure adequate storage for logs
Ensure that all systems that store logs have adequate storage space for the logs generated.

18.9.26.2.2 (L1) Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater' (Scored)

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: 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\EventLog\Security:MaxS
ize
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 196,608 or greater`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Event Log Service\Security\Specify the maximum log file size (KB)
```

Note: This Group Policy path is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.
Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Maximum Log Size (KB)*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Impact:

When event logs fill to capacity, they will stop recording information unless the retention method for each is set so that the computer will overwrite the oldest entries with the most recent ones. To mitigate the risk of loss of recent data, you can configure the retention method so that older events are overwritten as needed.

The consequence of this configuration is that older events will be removed from the logs. Attackers can take advantage of such a configuration, because they can generate a large number of extraneous events to overwrite any evidence of their attack. These risks can be somewhat reduced if you automate the archival and backup of event log data.

Ideally, all specifically monitored events should be sent to a server that uses Microsoft System Center Operations Manager (SCOM) or some other automated monitoring tool. Such a configuration is particularly important because an attacker who successfully compromises a server could clear the Security log. If all events are sent to a monitoring server, then you will be able to gather forensic information about the attacker's activities.

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.)

References:

1. CCE-37695-4

CIS Controls:

Version 6

6.3 Ensure Audit Logging Systems Are Not Subject To Loss (i.e. rotation/archive)
Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals. The logs must be archived and digitally signed on a periodic basis.

Version 7

6.4 Ensure adequate storage for logs
Ensure that all systems that store logs have adequate storage space for the logs generated.

18.9.26.3 Setup

This section contains recommendations for configuring the Setup Event Log.

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

18.9.26.3.1 (L1) Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\EventLog\Setup:Retenti
on
```

Remediation:

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

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

Note: This Group Policy path is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.
Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Retain old events*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Impact:

None - this is the default behavior.

Default Value:

Disabled. (When a log file reaches its maximum size, new events overwrite old events.)

References:

1. CCE-38276-2

CIS Controls:

Version 6

6.3 Ensure Audit Logging Systems Are Not Subject To Loss (i.e. rotation/archive)
Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals. The logs must be archived and digitally signed on a periodic basis.

Version 7

6.4 Ensure adequate storage for logs
Ensure that all systems that store logs have adequate storage space for the logs generated.

18.9.26.3.2 (L1) Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Scored)

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

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\EventLog\Setup:MaxSize
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 32,768 or greater`:

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

Note: This Group Policy path is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.
Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Maximum Log Size (KB)*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

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.

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.)

References:

1. CCE-37526-1

CIS Controls:

Version 6

6.3 Ensure Audit Logging Systems Are Not Subject To Loss (i.e. rotation/archive)
Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals. The logs must be archived and digitally signed on a periodic basis.

Version 7

6.4 Ensure adequate storage for logs
Ensure that all systems that store logs have adequate storage space for the logs generated.

18.9.26.4 System

This section contains recommendations for configuring the System Event Log.

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

18.9.26.4.1 (L1) Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\EventLog\System:Retent
ion
```

Remediation:

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

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

Note: This Group Policy path is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.
Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Retain old events*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Impact:

None - this is the default behavior.

Default Value:

Disabled. (When a log file reaches its maximum size, new events overwrite old events.)

References:

1. CCE-36160-0

CIS Controls:

Version 6

6.3 Ensure Audit Logging Systems Are Not Subject To Loss (i.e. rotation/archive)
Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals. The logs must be archived and digitally signed on a periodic basis.

Version 7

6.4 Ensure adequate storage for logs
Ensure that all systems that store logs have adequate storage space for the logs generated.

18.9.26.4.2 (L1) Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Scored)

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

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\EventLog\System:MaxSiz
e
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 32,768 or greater`:

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

Note: This Group Policy path is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.
Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Maximum Log Size (KB)*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Impact:

When event logs fill to capacity, they will stop recording information unless the retention method for each is set so that the computer will overwrite the oldest entries with the most recent ones. To mitigate the risk of loss of recent data, you can configure the retention method so that older events are overwritten as needed.

The consequence of this configuration is that older events will be removed from the logs. Attackers can take advantage of such a configuration, because they can generate a large number of extraneous events to overwrite any evidence of their attack. These risks can be somewhat reduced if you automate the archival and backup of event log data.

Ideally, all specifically monitored events should be sent to a server that uses Microsoft System Center Operations Manager (SCOM) or some other automated monitoring tool. Such a configuration is particularly important because an attacker who successfully compromises a server could clear the Security log. If all events are sent to a monitoring server, then you will be able to gather forensic information about the attacker's activities.

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.)

References:

1. CCE-36092-5

CIS Controls:

Version 6

6.3 Ensure Audit Logging Systems Are Not Subject To Loss (i.e. rotation/archive)
Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals. The logs must be archived and digitally signed on a periodic basis.

Version 7

6.4 Ensure adequate storage for logs
Ensure that all systems that store logs have adequate storage space for the logs generated.

18.9.27 Event Logging

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

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

18.9.28 Event Viewer

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

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

18.9.29 Family Safety (formerly Parental Controls)

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

This Group Policy section is provided by the Group Policy template `ParentalControls.admx/adml` that is only included with the Microsoft Windows Vista through the Windows 10 RTM (Release 1507) Administrative Templates.

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

18.9.30 File Explorer (formerly Windows Explorer)

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

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

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

18.9.30.1 (L1) Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Explorer:NoDataExecuti
onPrevention
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\File Explorer\Turn off Data Execution Prevention for Explorer
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Explorer.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Impact:

None - this is the default behavior.

Default Value:

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

References:

1. CCE-37809-1

CIS Controls:

Version 6

8.4 Enable Anti-exploitation Features (i.e. DEP, ASLR, EMET)

Enable anti-exploitation features such as Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualization/containerization, etc. For increased protection, deploy capabilities such as Enhanced Mitigation Experience Toolkit (EMET) that can be configured to apply these protections to a broader set of applications and executables.

Version 7

8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies

Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.

18.9.30.2 (L1) Ensure 'Turn off heap termination on corruption' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Explorer:NoHeapTermina
tionOnCorruption
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\File Explorer\Turn off heap termination on corruption
```

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

Impact:

None - this is the default behavior.

Default Value:

Disabled. (Heap termination on corruption is enabled.)

References:

1. CCE-36660-9

CIS Controls:

Version 6

8.4 Enable Anti-exploitation Features (i.e. DEP, ASLR, EMET)

Enable anti-exploitation features such as Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualization/containerization, etc. For increased protection, deploy capabilities such as Enhanced Mitigation Experience Toolkit (EMET) that can be configured to apply these protections to a broader set of applications and executables.

Version 7

8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies

Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.

18.9.30.3 (L1) Ensure 'Turn off shell protocol protected mode' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explore
r: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.

Impact:

None - this is the default behavior.

Default Value:

Disabled. (The protocol is in the protected mode, allowing applications to only open a limited set of folders.)

References:

1. CCE-36809-2

CIS Controls:

Version 6

8.4 Enable Anti-exploitation Features (i.e. DEP, ASLR, EMET)

Enable anti-exploitation features such as Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualization/containerization, etc. For increased protection, deploy capabilities such as Enhanced Mitigation Experience Toolkit (EMET) that can be configured to apply these protections to a broader set of applications and executables.

Version 7

8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies

Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.

18.9.31 File History

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

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

18.9.32 Find My Device

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

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

18.9.33 Game Explorer

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

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

18.9.34 Handwriting

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

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

18.9.35 HomeGroup

This section is 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).

18.9.36 Import Video

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

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

18.9.37 Internet Explorer

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

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

18.9.38 Internet Information Services

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

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

18.9.39 Location and Sensors

This section contains settings for Locations and Sensors.

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

18.9.39.1 Windows Location Provider

This section contains settings for Windows Location Provider.

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

18.9.39.1.1 (L2) Ensure 'Turn off Windows Location Provider' is set to 'Enabled' (Scored)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting turns off the Windows Location Provider feature for the computer.

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

Rationale:

This setting affects the Windows Location Provider 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\LocationAndSensors:Dis
ableWindowsLocationProvider
```

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\Windows Location Provider\Turn off Windows
Location Provider
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `LocationProviderAdm.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Impact:

The Windows Location Provider feature is turned off, and all programs on the computer are prevented from using the Windows Location Provider feature.

Default Value:

Disabled. (Programs on the computer are permitted to use the Windows Location Provider feature.)

References:

1. CCE-38225-9

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

18.9.39.2 (L2) Ensure 'Turn off location' is set to 'Enabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\LocationAndSensors:Dis
ableLocation
```

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).

Impact:

The location feature is turned off, and all programs on the computer are prevented from using location information from the location feature.

Default Value:

Disabled. (Programs on the computer are permitted to use location information from the location feature.)

References:

1. CCE-36886-0

CIS Controls:

Version 6

13 Data Protection
Data Protection

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

18.9.40 Maintenance Scheduler

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

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

18.9.41 Maps

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

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

18.9.42 MDM

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

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

18.9.43 Messaging

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

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

18.9.44 Microsoft account

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

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

18.9.45 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).

18.9.46 Microsoft FIDO Authentication

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

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

18.9.47 Microsoft Secondary Authentication Factor

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

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

18.9.48 Microsoft User Experience Virtualization

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

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

18.9.49 NetMeeting

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

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

18.9.50 Network Access Protection

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

This Group Policy section is provided by the Group Policy template `NAPXPQec.admx/adml` that is only included with the Microsoft Windows Server 2008 (non-R2) through the Windows 8.1 Update & Server 2012 R2 Update Administrative Templates.

18.9.51 Network Projector

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

This Group Policy section is provided by the Group Policy template `NetworkProjection.admx/adml` that is only included with the Microsoft Windows Vista through the Windows 8.1 Update & Server 2012 R2 Update Administrative Templates.

18.9.52 OneDrive (formerly SkyDrive)

This section contains recommendations related to OneDrive.

The Group Policy settings contained within this section are provided by the Group Policy template `SkyDrive.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

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

18.9.52.1 (L1) Ensure 'Prevent the usage of OneDrive for file storage' is set to 'Enabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\OneDrive:DisableFileSy
ncNGSC
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\OneDrive\Prevent the usage of OneDrive for file storage
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `SkyDrive.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer). However, we strongly recommend you only use the version included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer). Older versions of the templates had conflicting settings in different template files for both OneDrive & SkyDrive, until it was cleaned up properly in the above version.
Note #2: In older Microsoft Windows Administrative Templates, this setting was named *Prevent the usage of SkyDrive for file storage*, but it was renamed starting with the Windows 10 RTM (Release 1507) Administrative Templates.

Impact:

Users can't access OneDrive from the OneDrive app and file picker. Windows Store apps can't access OneDrive using the `WinRT` API. OneDrive doesn't appear in the navigation pane in File Explorer. OneDrive files aren't kept in sync with the cloud. Users can't automatically upload photos and videos from the camera roll folder.

Note: If your organization uses Office 365, be aware that this setting will prevent users from saving files to OneDrive/SkyDrive.

Note #2: If your organization has decided to implement **OneDrive for Business** and therefore needs to except itself from this recommendation, we highly suggest that you also obtain and utilize the `OneDrive.admx/adml` template that is bundled with the latest OneDrive client, as noted at this link (this template is not included with the Windows Administrative Templates). Two alternative OneDrive settings in particular from that template are worth your consideration:

- *Allow syncing OneDrive accounts for only specific organizations* - a computer-based setting that restricts OneDrive client connections to only **approved** tenant IDs.
- *Prevent users from synchronizing personal OneDrive accounts* - a user-based setting that prevents use of consumer OneDrive (i.e. non-business).

Default Value:

Disabled. (Apps and features can work with OneDrive file storage using the Next Generation Sync Client.)

References:

1. CCE-36939-7

CIS Controls:

Version 6

13 Data Protection
Data Protection

Version 7

13.4 Only Allow Access to Authorized Cloud Storage or Email Providers
Only allow access to authorized cloud storage or email providers.

18.9.52.2 (L1) Ensure 'Prevent the usage of OneDrive for file storage on Windows 8.1' is set to 'Enabled' (Scored)

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 legacy OneDrive/SkyDrive client.

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

Note: Despite the name of this setting, it is applicable to the legacy OneDrive client on any Windows OS.

Rationale:

Enabling this setting prevents users from accidentally (or intentionally) uploading confidential or sensitive corporate information to the OneDrive cloud service using the legacy OneDrive/SkyDrive 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\OneDrive:DisableFileSy
nc
```

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 on Windows
8.1
```

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 10 Release 1607 & Server 2016 Administrative Templates (or newer). We strongly recommend you only use either that version of the template or a newer one. 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.

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.

Default Value:

Disabled. (Apps and features can work with OneDrive file storage using the legacy OneDrive/SkyDrive client.)

References:

1. CCE-36939-7

CIS Controls:

Version 6

13 Data Protection
Data Protection

Version 7

13.4 Only Allow Access to Authorized Cloud Storage or Email Providers
Only allow access to authorized cloud storage or email providers.

18.9.53 Online Assistance

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

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

18.9.54 OOBE

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

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

18.9.55 Password Synchronization

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

This Group Policy section is provided by the Group Policy template `PswdSync.admx/adml` that is only included with the Microsoft Windows Vista through the Windows 8.1 Update & Server 2012 R2 Update Administrative Templates.

18.9.56 Portable Operating System

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

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

18.9.57 Presentation Settings

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

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

18.9.58 Push To Install

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

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

18.9.59 Remote Desktop Services (formerly Terminal Services)

This section contains recommendations related to Remote Desktop Services.

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

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

18.9.59.1 RD Licensing (formerly TS Licensing)

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

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

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

18.9.59.2 Remote Desktop Connection Client

This section contains recommendations for the Remote Desktop Connection Client.

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

18.9.59.2.1 RemoteFX USB Device Redirection

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

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

18.9.59.2.2 (L1) Ensure 'Do not allow passwords to be saved' is set to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services:DisablePasswordSaving
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Remote Desktop Services\Remote Desktop Connection Client\Do not
allow passwords to be saved
```

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

Impact:

The password saving checkbox will be disabled for Remote Desktop clients and users will not be able to save passwords.

Default Value:

Disabled. (Users will be able to save passwords using Remote Desktop Connection.)

References:

1. CCE-36223-6

CIS Controls:

Version 6

16.4 Automatically Log Off Users After Standard Period Of Inactivity
Regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.

Version 7

16.11 Lock Workstation Sessions After Inactivity
Automatically lock workstation sessions after a standard period of inactivity.

18.9.59.3 Remote Desktop Session Host (formerly Terminal Server)

This section contains recommendations for the Remote Desktop Session Host.

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

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

18.9.59.3.1 Application Compatibility

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

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

18.9.59.3.2 Connections

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

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

18.9.59.3.2.1 (L2) Ensure 'Restrict Remote Desktop Services users to a single Remote Desktop Services session' is set to 'Enabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services: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.

Impact:

None - this is the default behavior.

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.)

References:

1. CCE-37708-5

CIS Controls:

Version 7

4.5 Use Multifactor Authentication For All Administrative Access
Use multi-factor authentication and encrypted channels for all administrative account access.

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

18.9.59.3.3 Device and Resource Redirection

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

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

18.9.59.3.3.1 (L2) Ensure 'Do not allow COM port redirection' is set to 'Enabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services:fDisableCcm
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Remote Desktop Services\Remote Desktop Session Host\Device and
Resource Redirection\Do not allow COM port redirection
```

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

Impact:

Users in a Remote Desktop Services session will not be able to redirect server data to local (client) COM ports.

Default Value:

Disabled. (Remote Desktop Services allows COM port redirection.)

References:

1. CCE-37696-2

CIS Controls:

Version 6

9.1 Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

18.9.59.3.3.2 (L1) Ensure 'Do not allow drive redirection' is set to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services:fDisableCdm
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Remote Desktop Services\Remote Desktop Session Host\Device and
Resource Redirection\Do not allow drive redirection
```

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

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.

Default Value:

Disabled. (An RD Session Host maps client drives automatically upon connection.)

References:

1. CCE-36509-8

CIS Controls:

Version 6

13 Data Protection
Data Protection

Version 7

14.6 Protect Information through Access Control Lists
Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

18.9.59.3.3.3 (L2) Ensure 'Do not allow LPT port redirection' is set to 'Enabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services:fDisableLPT
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Remote Desktop Services\Remote Desktop Session Host\Device and
Resource Redirection\Do not allow LPT port redirection
```

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

Impact:

Users in a Remote Desktop Services session will not be able to redirect server data to local (client) LPT ports.

Default Value:

Disabled. (Remote Desktop Services allows LPT port redirection.)

References:

1. CCE-37778-8

CIS Controls:

Version 6

9.1 Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

18.9.59.3.3.4 (L2) Ensure 'Do not allow supported Plug and Play device redirection' is set to 'Enabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services:fDisablePNPRedir
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Remote Desktop Services\Remote Desktop Session Host\Device and
Resource Redirection\Do not allow supported Plug and Play device redirection
```

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

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.

Default Value:

Disabled. (Remote Desktop Services allows redirection of supported Plug and Play devices.)

References:

1. CCE-37477-7

CIS Controls:

Version 6

9.1 Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

18.9.59.3.4 Licensing

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

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

18.9.59.3.5 Printer Redirection

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

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

18.9.59.3.6 Profiles

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

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

18.9.59.3.7 RD Connection Broker (formerly TS Connection Broker)

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note: This section was initially named *TS Connection Broker* but was renamed by Microsoft to *RD Connection Broker* starting with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates.

18.9.59.3.8 Remote Session Environment

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.59.3.9 Security

This section contains recommendations related to Remote Desktop Session Host Security.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.59.3.9.1 (L1) Ensure 'Always prompt for password upon connection' is set to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services:fPromptForPassword
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Remote Desktop Services\Remote Desktop Session
Host\Security\Always prompt for password upon connection
```

Note: This Group Policy path is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.
Note #2: In the Microsoft Windows Vista Administrative Templates, this setting was named *Always prompt client for password upon connection*, but it was renamed starting with the Windows Server 2008 (non-R2) Administrative Templates.

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.

Default Value:

Disabled. (Remote Desktop Services allows users to automatically log on if they enter a password in the Remote Desktop Connection client.)

References:

1. CCE-37929-7

CIS Controls:

Version 6

16.14 Encrypt/Hash All Authentication Files And Monitor Their Access

Verify that all authentication files are encrypted or hashed and that these files cannot be accessed without root or administrator privileges. Audit all access to password files in the system.

Version 7

16.4 Encrypt or Hash all Authentication Credentials

Encrypt or hash with a salt all authentication credentials when stored.

16.5 Encrypt Transmittal of Username and Authentication Credentials

Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.

18.9.59.3.9.2 (L1) Ensure 'Require secure RPC communication' is set to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services:fEncryptRPCTraffic
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Remote Desktop Services\Remote Desktop Session
Host\Security\Require secure RPC communication
```

Note: This Group Policy path is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Impact:

Remote Desktop Services accepts requests from RPC clients that support secure requests, and does not allow unsecured communication with untrusted clients.

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.)

References:

1. CCE-37567-5

CIS Controls:

Version 6

3.4 Use Only Secure Channels For Remote System Administration

Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.

Version 7

4.5 Use Multifactor Authentication For All Administrative Access

Use multi-factor authentication and encrypted channels for all administrative account access.

18.9.59.3.9.3 (L1) Ensure 'Require use of specific security layer for remote (RDP) connections' is set to 'Enabled: SSL' (Scored)

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 labelled *SSL*, it is actually enforcing Transport Layer Security (TLS) version 1.0, not the older (and less secure) SSL protocol.

Rationale:

The native Remote Desktop Protocol (RDP) encryption is now considered a weak protocol, so enforcing the use of stronger Transport Layer Security (TLS) encryption for all RDP communications between clients and RD Session Host servers is preferred.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services:SecurityLayer
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: SSL`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Remote Desktop Services\Remote Desktop Session
Host\Security\Require use of specific security layer for remote (RDP)
connections
```

Note: This Group Policy path is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

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.

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.)

References:

1. CCE-36598-1

CIS Controls:

Version 6

3.4 Use Only Secure Channels For Remote System Administration

Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.

Version 7

4.5 Use Multifactor Authentication For All Administrative Access

Use multi-factor authentication and encrypted channels for all administrative account access.

18.9.59.3.9.4 (L1) Ensure 'Require user authentication for remote connections by using Network Level Authentication' is set to 'Enabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services:UserAuthentication
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Remote Desktop Services\Remote Desktop Session
Host\Security\Require user authentication for remote connections by using
Network Level Authentication
```

Note: This Group Policy path is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.
Note #2: In the Microsoft Windows Vista Administrative Templates, this setting was initially named *Require user authentication using RDP 6.0 for remote connections*, but it was renamed starting with the Windows Server 2008 (non-R2) Administrative Templates.

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.

Default Value:

Windows Server 2008 R2 and older: Disabled.

Windows Server 2012 (non-R2) and newer: Enabled.

References:

1. CCE-37330-8

CIS Controls:

Version 6

3.4 Use Only Secure Channels For Remote System Administration

Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.

Version 7

4.5 Use Multifactor Authentication For All Administrative Access

Use multi-factor authentication and encrypted channels for all administrative account access.

18.9.59.3.9.5 (L1) Ensure 'Set client connection encryption level' is set to 'Enabled: High Level' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services:MinEncryptionLevel
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: High Level`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Remote Desktop Services\Remote Desktop Session Host\Security\Set
client connection encryption level
```

Note: This Group Policy path is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Impact:

None - this is the default behavior.

Default Value:

Enabled: High Level. (All communications between clients and RD Session Host servers during remote connections using native RDP encryption must be 128-bit strength. Clients that do not support 128-bit encryption will be unable to establish Remote Desktop Server sessions.)

References:

1. CCE-36627-8

CIS Controls:

Version 6

3.4 Use Only Secure Channels For Remote System Administration

Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.

Version 7

4.5 Use Multifactor Authentication For All Administrative Access

Use multi-factor authentication and encrypted channels for all administrative account access.

18.9.59.3.10 Session Time Limits

This section contains recommendations related to Remote Desktop Session Host Session Time Limits.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.59.3.10.1 (L2) Ensure 'Set time limit for active but idle Remote Desktop Services sessions' is set to 'Enabled: 15 minutes or less' (Scored)

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.`

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services:MaxIdleTime
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 15 minutes or less:`

```
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.

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.

Default Value:

Disabled. (Remote Desktop Services allows sessions to remain active but idle for an unlimited amount of time.)

References:

1. CCE-37562-6

CIS Controls:

Version 6

16.5 Ensure Workstation Screen Locks Are Configured
Configure screen locks on systems to limit access to unattended workstations.

Version 7

16.11 Lock Workstation Sessions After Inactivity
Automatically lock workstation sessions after a standard period of inactivity.

18.9.59.3.10.2 (L2) Ensure 'Set time limit for disconnected sessions' is set to 'Enabled: 1 minute' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services:MaxDisconnectionTime
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 1 minute`:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Session Time Limits\Set time limit for disconnected sessions
```

Note: This Group Policy path is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

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.

Default Value:

Disabled. (Disconnected Remote Desktop sessions are maintained for an unlimited time on the server.)

References:

1. CCE-37949-5

CIS Controls:

Version 6

16.5 Ensure Workstation Screen Locks Are Configured
Configure screen locks on systems to limit access to unattended workstations.

Version 7

16.11 Lock Workstation Sessions After Inactivity
Automatically lock workstation sessions after a standard period of inactivity.

18.9.59.3.11 Temporary folders

This section contains recommendations related to Remote Desktop Session Host Session Temporary folders.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.59.3.11.1 (L1) Ensure 'Do not delete temp folders upon exit' is set to 'Disabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services:DeleteTempDirsOnExit
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Remote Desktop Services\Remote Desktop Session Host\Temporary
Folders\Do not delete temp folders upon exit
```

Note: This Group Policy path is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.
Note #2: In older Microsoft Windows Administrative Templates, this setting was named *Do not delete temp folder upon exit*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Impact:

None - this is the default behavior.

Default Value:

Disabled. (Temporary folders are deleted when a user logs off.)

References:

1. CCE-37946-1

CIS Controls:

Version 6

14.4 Protect Information With Access Control Lists
All information stored on systems shall be protected 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.

Version 7

14.6 Protect Information through Access Control Lists
Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

18.9.59.3.11.2 (L1) Ensure 'Do not use temporary folders per session' is set to 'Disabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services: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.

Impact:

None - this is the default behavior.

Default Value:

Disabled. (Per-session temporary folders are created.)

References:

1. CCE-38180-6

CIS Controls:

Version 6

14.4 Protect Information With Access Control Lists
All information stored on systems shall be protected 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.

Version 7

14.6 Protect Information through Access Control Lists
Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

18.9.60 RSS Feeds

This section contains recommendations related to RSS feeds.

This Group Policy section is provided by the Group Policy template `InetRes.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.60.1 (L1) Ensure 'Prevent downloading of enclosures' is set to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet
Explorer\Feeds:DisableEnclosureDownload
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\RSS Feeds\Prevent downloading of enclosures
```

Note: This Group Policy path is provided by the Group Policy template `InetRes.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.
Note #2: In older Microsoft Windows Administrative Templates, this setting was named *Turn off downloading of enclosures*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

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.

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.)

References:

1. CCE-37126-0

CIS Controls:

Version 6

7.2 Uninstall/Disable Unnecessary or Unauthorized Browser Or Email Client Plugins
Uninstall or disable any unnecessary or unauthorized browser or email client plugins or add-on applications. Each plugin shall utilize application / URL whitelisting and only allow the use of the application for pre-approved domains.

Version 7

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.

18.9.61 Search

This section contains recommendations for Search settings.

This Group Policy section is provided by the Group Policy template `Search.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.61.2 (L1) Ensure 'Allow indexing of encrypted files' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows
Search:AllowIndexingEncryptedStoresOrItems
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Search\Allow indexing of encrypted files
```

Note: This Group Policy path is provided by the Group Policy template `Search.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Impact:

None - this is the default behavior.

Default Value:

Disabled. (Search service components (including non-Microsoft components) are expected not to index encrypted items or encrypted stores.)

References:

1. CCE-38277-0

CIS Controls:

Version 6

13.1 Assess Data To Identify Sensitive Information
Perform an assessment of data to identify sensitive information that requires the application of encryption and integrity controls.

Version 7

13.3 Monitor and Block Unauthorized Network Traffic
Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.

18.9.62 Security Center

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `SecurityCenter.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.63 Server for NIS

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Snis.admx/adml` that is only included with the Microsoft Windows Vista through the Windows 8.1 Update & Server 2012 R2 Update Administrative Templates.

18.9.64 Shutdown Options

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WinInit.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.65 Smart Card

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `SmartCard.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.66 Software Protection Platform

This section contains recommendations related to the Software Protection Platform.

This Group Policy section is provided by the Group Policy template `AVSValidationGP.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

18.9.66.1 (L2) Ensure 'Turn off KMS Client Online AVS Validation' is set to 'Enabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows
NT\CurrentVersion\Software Protection Platform:NoGenTicket
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Software Protection Platform\Turn off KMS Client Online AVS
Validation
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `AVSValidationGP.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

Impact:

The computer is prevented from sending data to Microsoft regarding its KMS client activation state.

Default Value:

Disabled. (KMS client activation data will automatically be sent to Microsoft when the device activates.)

CIS Controls:

Version 7

13.3 Monitor and Block Unauthorized Network Traffic
Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.

18.9.67 Sound Recorder

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `SoundRec.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.68 Speech

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Speech.admx/adml` that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

18.9.69 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).

18.9.70 Sync your settings

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `SettingSync.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.9.71 Tablet PC

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.72 Task Scheduler

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `TaskScheduler.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.73 Text Input

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `TextInput.admx/adml` that is only included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates and Microsoft Windows 10 Release 1511 Administrative Templates.

18.9.74 Windows Calendar

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WinCal.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.75 Windows Color System

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsColorSystem.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.76 Windows Customer Experience Improvement Program

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `CEIPEnable.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.77 Windows Defender Antivirus (formerly Windows Defender)

This section contains recommendations related to Windows Defender Antivirus.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note: This section was originally named *Windows Defender* but was renamed by Microsoft to *Windows Defender Antivirus* starting with the Microsoft Windows 10 Release 1703 Administrative Templates.

18.9.77.1 Client Interface

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.77.2 Exclusions

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.77.3 MAPS

This section contains recommendations related to Microsoft Active Protection Service (MAPS).

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.77.3.1 (L1) Ensure 'Configure local setting override for reporting to Microsoft MAPS' is set to 'Disabled' (Scored)

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 "Windows Defender Antivirus Cloud Protection Service". This setting can only be set by Group Policy.

The recommended state for this setting is: `Disabled`.

Rationale:

The decision on whether or not to participate in Microsoft MAPS / Windows Defender Antivirus Cloud Protection Service for malicious software reporting should be made centrally in an enterprise managed environment, so that all computers within it behave consistently in that regard. Configuring this setting to Disabled ensures that the decision remains centrally managed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows
Defender\Spynet:LocalSettingOverrideSpynetReporting
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Defender Antivirus\MAPS\Configure local setting override
for reporting to Microsoft MAPS
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Impact:

None - this is the default behavior.

Default Value:

Disabled. (Group Policy will take priority over the local preference setting.)

References:

1. CCE-36940-5

CIS Controls:

Version 6

8 Malware Defenses
Malware Defenses

Version 7

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.

8.1 Utilize Centrally Managed Anti-malware Software
Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.

8.2 Ensure Anti-Malware Software and Signatures are Updated
Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.

18.9.77.3.2 (L2) Ensure 'Join Microsoft MAPS' is set to 'Disabled' (Scored)

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". Microsoft MAPS / Windows Defender Antivirus Cloud Protection Service is the online community that helps you choose how to respond to potential threats. The community also helps stop the spread of new malicious software infections. You can choose to send basic or additional information about detected software. Additional information helps Microsoft create new definitions and help it to protect your computer.

Possible options are:

- (0x0) Disabled (default)
- (0x1) Basic membership
- (0x2) Advanced membership

Basic membership will send basic information to Microsoft about software that has been detected including where the software came from the actions that you apply or that are applied automatically and whether the actions were successful.

Advanced membership in addition to basic information will send more information to Microsoft about malicious software spyware and potentially unwanted software including the location of the software file names how the software operates and how it has impacted your computer.

The recommended state for this setting is: `Disabled`.

Rationale:

The information that would be sent can include things like location of detected items on your computer if harmful software was removed. The information would be automatically collected and sent. In some instances personal information might unintentionally be sent to Microsoft. However, Microsoft states that it will not use this information to identify you or contact you.

For privacy reasons in high security environments, it is best to prevent these data submissions altogether.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is in effect when the following registry value does not exist, or when it exists with a value of `0`:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows
Defender\Spynet:SpynetReporting
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows 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).

Impact:

None - this is the default behavior.

Default Value:

Disabled. (Microsoft MAPS / Windows Defender Antivirus Cloud Protection Service will not be joined.)

CIS Controls:

Version 7

13.3 Monitor and Block Unauthorized Network Traffic

Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.

18.9.77.4 MpEngine

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

18.9.77.5 Network Inspection System

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.77.6 Quarantine

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.77.7 Real-time Protection

This section contains settings related to Real-time Protection.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.77.7.1 (L1) Ensure 'Turn on behavior monitoring' is set to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to configure behavior monitoring for Windows Defender Antivirus.

The recommended state for this setting is: `Enabled`.

Rationale:

When running an antivirus solution such as Windows Defender Antivirus, it is important to ensure that it is configured to heuristically monitor in real-time for suspicious and known malicious activity.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time
Protection:DisableBehaviorMonitoring
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Defender Antivirus\Real-Time Protection\Turn on behavior
monitoring
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Impact:

None - this is the default configuration.

Default Value:

Enabled. (Behavior monitoring will be enabled.)

References:

1. CCE-38389-3

CIS Controls:

Version 6

8.1 Deploy Automated Endpoint Protection Tools
Employ automated tools to continuously monitor workstations, servers, and mobile devices with anti-virus, anti-spyware, personal firewalls, and host-based IPS functionality. All malware detection events should be sent to enterprise anti-malware administration tools and event log servers.

Version 7

8.1 Utilize Centrally Managed Anti-malware Software
Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.

8.2 Ensure Anti-Malware Software and Signatures are Updated
Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.

8.6 Centralize Anti-malware Logging
Send all malware detection events to enterprise anti-malware administration tools and event log servers for analysis and alerting.

18.9.77.8 Remediation

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.77.9 Reporting

This section contains settings related to Windows Defender Reporting.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.77.9.1 (L2) Ensure 'Configure Watson events' is set to 'Disabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows
Defender\Reporting:DisableGenericRePorts
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows 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).

Impact:

Watson events will not be sent to Microsoft automatically when a program or service crashes or fails.

Default Value:

Enabled. (Watson events *will* be sent to Microsoft automatically when a program or service crashes or fails.)

References:

1. CCE-36950-4

CIS Controls:

Version 6

13 Data Protection
Data Protection

Version 7

13.3 Monitor and Block Unauthorized Network Traffic
Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.

18.9.77.10 Scan

This section contains settings related to Windows Defender scanning.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.77.10.1 (L1) Ensure 'Scan removable drives' is set to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to manage whether or not to scan for malicious software and unwanted software in the contents of removable drives, such as USB flash drives, when running a full scan.

The recommended state for this setting is: `Enabled`.

Rationale:

It is important to ensure that any present removable drives are always included in any type of scan, as removable drives are more likely to contain malicious software brought in to the enterprise managed environment from an external, unmanaged computer.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows
Defender\Scan:DisableRemovableDriveScanning
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Defender Antivirus\Scan\Scan removable drives
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Impact:

Removable drives will be scanned during any type of scan by Windows Defender Antivirus.

Default Value:

Disabled. (Removable drives will not be scanned during a full scan. Removable drives may still be scanned during quick scan and custom scan.)

References:

1. CCE-38409-9

CIS Controls:

Version 6

13 Data Protection
Data Protection

Version 7

8.4 Configure Anti-Malware Scanning of Removable Devices
Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.

18.9.77.10.2 (L1) Ensure 'Turn on e-mail scanning' is set to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to configure e-mail scanning. When e-mail scanning is enabled, the engine will parse the mailbox and mail files, according to their specific format, in order to analyze the mail bodies and attachments. Several e-mail formats are currently supported, for example: pst (Outlook), dbx, mbx, mime (Outlook Express), binhex (Mac).

The recommended state for this setting is: `Enabled`.

Rationale:

Incoming e-mails should be scanned by an antivirus solution such as Windows Defender Antivirus, as email attachments are a commonly used attack vector to infiltrate computers with malicious software.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows
Defender\Scan:DisableEmailScanning
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Defender Antivirus\Scan\Turn on e-mail scanning
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Impact:

E-mail scanning by Windows Defender Antivirus will be enabled.

Default Value:

Disabled. (E-mail scanning by Windows Defender Antivirus will be disabled.)

References:

1. CCE-36958-7

CIS Controls:

Version 6

13 Data Protection
Data Protection

Version 7

8.1 Utilize Centrally Managed Anti-malware Software
Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.

8.2 Ensure Anti-Malware Software and Signatures are Updated
Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.

18.9.77.11 Security Intelligence Updates (formerly Signature Updates)

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Note: This section was initially named *Signature Updates* but was renamed by Microsoft to *Security Intelligence Updates* starting with the Microsoft Windows 10 Release 1903 Administrative Templates.

18.9.77.12 Threats

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.77.13 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 `WindowsDefender.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

18.9.77.14 (L1) Ensure 'Turn off Windows Defender AntiVirus' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting turns off Windows Defender Antivirus. If the setting is configured to Disabled, Windows Defender Antivirus runs and computers are scanned for malware and other potentially unwanted software.

The recommended state for this setting is: `Disabled`.

Rationale:

It is important to ensure a current, updated antivirus product is scanning each computer for malicious file activity. Microsoft provides a competent solution out of the box in Windows Defender Antivirus.

Organizations that choose to purchase a reputable 3rd-party antivirus solution may choose to exempt themselves from this recommendation in lieu of the commercial alternative.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows
Defender:DisableAntiSpyware
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Defender Antivirus\Turn off Windows Defender AntiVirus
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.
Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Turn off Windows Defender*, but it was renamed starting with the Windows 10 Release 1703 Administrative Templates.

Impact:

None - this is the default behavior.

Default Value:

Disabled. (Windows Defender Antivirus runs and computers are scanned for malware and other potentially unwanted software.)

References:

1. CCE-36082-6

CIS Controls:

Version 6

8.1 Deploy Automated Endpoint Protection Tools

Employ automated tools to continuously monitor workstations, servers, and mobile devices with anti-virus, anti-spyware, personal firewalls, and host-based IPS functionality. All malware detection events should be sent to enterprise anti-malware administration tools and event log servers.

Version 7

8.1 Utilize Centrally Managed Anti-malware Software

Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.

8.2 Ensure Anti-Malware Software and Signatures are Updated

Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.

18.9.78 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).

18.9.79 Windows Defender Exploit Guard

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `ExploitGuard.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

18.9.80 Windows Defender SmartScreen

This section contains Windows Defender SmartScreen settings.

This Group Policy section is provided by the Group Policy template `SmartScreen.admx/adml` that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

18.9.80.1 Explorer

This section contains recommendations for Explorer-related Windows Defender SmartScreen settings.

The Group Policy settings contained within this section are provided by the Group Policy template `WindowsExplorer.admx/adml` that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

18.9.80.1.1 (L1) Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled: Warn and prevent bypass' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry locations:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System:EnableSmartScre
en
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System:ShellSmartScree
nLevel
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Warn and prevent bypass:`

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Defender SmartScreen\Explorer\Configure Windows Defender
SmartScreen
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsExplorer.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).
Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Configure Windows SmartScreen*, but it was renamed starting with the Windows 10 Release 1703 Administrative Templates.

Impact:

Users will be warned before they are allowed to run unrecognized programs downloaded from the Internet.

Default Value:

Disabled. (Windows SmartScreen behavior is managed by administrators on the PC by using Windows SmartScreen Settings in Action Center.)

References:

1. CCE-35859-8

CIS Controls:

Version 6

2 Inventory of Authorized and Unauthorized Software
Inventory of Authorized and Unauthorized Software

Version 7

2.6 Address unapproved software
Ensure that unauthorized software is either removed or the inventory is updated in a timely manner

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.

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.

7.3 Limit Use of Scripting Languages in Web Browsers and Email Clients
Ensure that only authorized scripting languages are able to run in all web browsers and email clients.

18.9.81 Windows Error Reporting

This section contains recommendations related to Windows Error Reporting.

This Group Policy section is provided by the Group Policy template `ErrorReporting.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.81.1 Advanced Error Reporting 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 `ErrorReporting.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.81.2 Consent

This section contains recommendations related to Windows Error Reporting consent.

This Group Policy section is provided by the Group Policy template `ErrorReporting.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.81.2.1 (L1) Ensure 'Configure Default consent' is set to 'Enabled: Always ask before sending data' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This setting allows you to set the default consent handling for error reports.

The recommended state for this setting is: `Enabled: Always ask before sending data`

Rationale:

Error reports may contain sensitive information and should not be sent to anyone automatically.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows Error
Reporting\Consent:DefaultConsent
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`: `Always ask before sending data`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Error Reporting\Consent\Configure Default consent
```

Note: This Group Policy path is provided by the Group Policy template `ErrorReporting.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Impact:

None - this is the default behavior.

Default Value:

Always ask before sending data. (Windows prompts users for consent to send reports.)

References:

1. CCE-37112-0

CIS Controls:

Version 6

13 Data Protection
Data Protection

Version 7

13.3 Monitor and Block Unauthorized Network Traffic
Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.

18.9.82 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).

18.9.83 Windows Hello for Business (formerly Microsoft Passport for Work)

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Passport.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

Note: This section was initially named *Microsoft Passport for Work* but was renamed by Microsoft to *Windows Hello for Business* starting with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates.

18.9.84 Windows Ink Workspace

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsInkWorkspace.admx/adml` that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

18.9.85 Windows Installer

This section contains recommendations related to Windows Installer.

This Group Policy section is provided by the Group Policy template `MSI.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.85.1 (L1) Ensure 'Allow user control over installs' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer:EnableUserCo
ntrol
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Installer\Allow user control over installs
```

Note: This Group Policy path is provided by the Group Policy template `MSI.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.
Note #2: In older Microsoft Windows Administrative Templates, this setting was named *Enable user control over installs*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Impact:

None - this is the default behavior.

Default Value:

Disabled. (The security features of Windows Installer will prevent users from changing installation options typically reserved for system administrators, such as specifying the directory to which files are installed.)

References:

1. CCE-36400-0

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

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.

4.6 Use of Dedicated Machines For All Administrative Tasks

Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.

18.9.85.2 (L1) Ensure 'Always install with elevated privileges' is set to 'Disabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer:AlwaysInstal
lElevated
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Installer\Always install with elevated privileges
```

Note: This Group Policy path is provided by the Group Policy template `MSI.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Impact:

None - this is the default behavior.

Default Value:

Disabled. (Windows Installer will apply the current user's permissions when it installs programs that a system administrator does not distribute or offer. This will prevent standard users from installing applications that affect system-wide configuration items.)

References:

1. CCE-36919-9

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

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.

4.6 Use of Dedicated Machines For All Administrative Tasks
Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.

18.9.85.3 (L2) Ensure 'Prevent Internet Explorer security prompt for Windows Installer scripts' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer:SafeForScrip
ting
```

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.

Impact:

None - this is the default behavior.

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.)

References:

1. CCE-37524-6

CIS Controls:

Version 6

7 Email and Web Browser Protections
Email and Web Browser Protections

Version 7

7.3 Limit Use of Scripting Languages in Web Browsers and Email Clients
Ensure that only authorized scripting languages are able to run in all web browsers and email clients.

18.9.86 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.

18.9.87 Windows Mail

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsMail.admx/adml` that is only included with the Microsoft Windows Vista through the Windows 10 Release 1703 Administrative Templates.

18.9.88 Windows Media Center

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `MediaCenter.admx/adml` that is only included with the Microsoft Windows Vista through Windows 10 Release 1511 Administrative Templates.

18.9.89 Windows Media Digital Rights Management

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsMediaDRM.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.90 Windows Media Player

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsMediaPlayer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.91 Windows Meeting Space

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsCollaboration.admx/adml` that is only included with the Microsoft Windows Vista and Server 2008 (non-R2) Administrative Templates.

18.9.92 Windows Messenger

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsMessenger.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.93 Windows Mobility Center

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `MobilePCMobilityCenter.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.94 Windows Movie Maker

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `MovieMaker.admx/adml` that is only included with the Microsoft Windows Vista and Server 2008 (non-R2) Administrative Templates.

18.9.95 Windows PowerShell

This section contains recommendations related to Windows PowerShell.

This Group Policy section is provided by the Group Policy template `PowerShellExecutionPolicy.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.9.95.1 (L1) Ensure 'Turn on PowerShell Script Block Logging' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting enables logging of all PowerShell script input to the Microsoft-Windows-PowerShell/Operational event log.

The recommended state for this setting is: `Disabled`.

Note: In Microsoft's own hardening guidance, they recommend the opposite value, `Enabled`, because having this data logged improves investigations of PowerShell attack incidents. However, the default ACL on the PowerShell Operational log allows Interactive User (i.e. *any* logged on user) to read it, and therefore possibly expose passwords or other sensitive information to unauthorized users. If Microsoft locks down the default ACL on that log in the future (e.g. to restrict it only to Administrators), then we will revisit this recommendation in a future release.

Rationale:

There are potential risks of capturing passwords in the PowerShell logs. This setting should only be needed for debugging purposes, and not in normal operation, it is important to ensure this is set to `Disabled`.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlock
Logging:EnableScriptBlockLogging
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows PowerShell\Turn on PowerShell Script Block Logging
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `PowerShellExecutionPolicy.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

Impact:

Logging of PowerShell script input is disabled.

Default Value:

Enabled. (PowerShell will log script blocks the first time they are used.)

CIS Controls:

Version 6

16.4 Automatically Log Off Users After Standard Period Of Inactivity
Regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

18.9.95.2 (L1) Ensure 'Turn on PowerShell Transcription' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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: `Disabled`.

Rationale:

If this setting is enabled there is a risk that passwords could get stored in plain text in the `PowerShell_transcript` output file.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\PowerShell\Transcripti
on:EnableTranscripting
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows PowerShell\Turn on PowerShell Transcription
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `PowerShellExecutionPolicy.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

Impact:

None - this is the default behavior.

Default Value:

Disabled. (Transcription of PowerShell-based applications is disabled by default, although transcription can still be enabled through the `Start-Transcript` cmdlet.)

CIS Controls:

Version 6

16.4 Automatically Log Off Users After Standard Period Of Inactivity
Regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

18.9.96 Windows Reliability Analysis

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `RacWmiProv.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.9.97 Windows Remote Management (WinRM)

This section contains recommendations related to Windows Remote Management (WinRM).

This Group Policy section is provided by the Group Policy template `WindowsRemoteManagement.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.97.1 WinRM Client

This section contains recommendations related to the Windows Remote Management (WinRM) client.

This Group Policy section is provided by the Group Policy template `WindowsRemoteManagement.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.97.1.1 (L1) Ensure 'Allow Basic authentication' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WinRM\Client:AllowBasi
c
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Remote Management (WinRM)\WinRM Client\Allow Basic
authentication
```

Note: This Group Policy path is provided by the Group Policy template `WindowsRemoteManagement.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Impact:

None - this is the default behavior.

Default Value:

Disabled. (The WinRM client does not use Basic authentication.)

References:

1. CCE-36310-1

CIS Controls:

Version 6

16.13 User/Account Authentication Must Be Performed Over Encrypted Channels

Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.

Version 7

14.4 Encrypt All Sensitive Information in Transit

Encrypt all sensitive information in transit.

16.5 Encrypt Transmittal of Username and Authentication Credentials

Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.

18.9.97.1.2 (L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WinRM\Client:AllowUnen
cryptedTraffic
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Remote Management (WinRM)\WinRM Client\Allow unencrypted
traffic
```

Note: This Group Policy path is provided by the Group Policy template `WindowsRemoteManagement.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Impact:

None - this is the default behavior.

Default Value:

Disabled. (The WinRM client sends or receives only encrypted messages over the network.)

References:

1. CCE-37726-7

CIS Controls:

Version 6

16.13 User/Account Authentication Must Be Performed Over Encrypted Channels
Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.

Version 7

14.4 Encrypt All Sensitive Information in Transit
Encrypt all sensitive information in transit.

16.5 Encrypt Transmittal of Username and Authentication Credentials
Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.

18.9.97.1.3 (L1) Ensure 'Disallow Digest authentication' is set to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WinRM\Client:AllowDige
st
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Remote Management (WinRM)\WinRM Client\Disallow Digest
authentication
```

Note: This Group Policy path is provided by the Group Policy template `WindowsRemoteManagement.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Impact:

The WinRM client will not use Digest authentication.

Default Value:

Disabled. (The WinRM client will use Digest authentication.)

References:

1. CCE-38318-2

CIS Controls:

Version 6

16.13 User/Account Authentication Must Be Performed Over Encrypted Channels
Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.

Version 7

14.4 Encrypt All Sensitive Information in Transit
Encrypt all sensitive information in transit.

16.5 Encrypt Transmittal of Username and Authentication Credentials
Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.

18.9.97.2 WinRM Service

This section contains recommendations related to the Windows Remote Management (WinRM) service.

This Group Policy section is provided by the Group Policy template `WindowsRemoteManagement.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.97.2.1 (L1) Ensure 'Allow Basic authentication' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WinRM\Service:AllowBas
ic
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Remote Management (WinRM)\WinRM Service\Allow Basic
authentication
```

Note: This Group Policy path is provided by the Group Policy template `WindowsRemoteManagement.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Impact:

None - this is the default behavior.

Default Value:

Disabled. (The WinRM service will not accept Basic authentication from a remote client.)

References:

1. CCE-36254-1

CIS Controls:

Version 6

16.13 User/Account Authentication Must Be Performed Over Encrypted Channels
Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.

Version 7

14.4 Encrypt All Sensitive Information in Transit
Encrypt all sensitive information in transit.

16.5 Encrypt Transmittal of Username and Authentication Credentials
Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.

18.9.97.2.2 (L2) Ensure 'Allow remote server management through WinRM' is set to 'Disabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy object is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WinRM\Service:AllowAut
oConfig
```

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.

Impact:

None - this is the default behavior.

Default Value:

Disabled. (The WinRM service will not respond to requests from a remote computer, regardless of whether or not any WinRM listeners are configured.)

References:

1. CCE-37927-1

CIS Controls:

Version 6

3.4 Use Only Secure Channels For Remote System Administration

Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.

9.3 Perform Regular Automated Port Scanning

Perform automated port scans on a regular basis against all key servers and compare to a known effective baseline. If a change that is not listed on the organization's approved baseline is discovered, an alert should be generated and reviewed.

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

18.9.97.2.3 (L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WinRM\Service:AllowUne
ncryptedTraffic
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Remote Management (WinRM)\WinRM Service\Allow unencrypted
traffic
```

Note: This Group Policy path is provided by the Group Policy template `WindowsRemoteManagement.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Impact:

None - this is the default behavior.

Default Value:

Disabled. (The WinRM service sends or receives only encrypted messages over the network.)

References:

1. CCE-38223-4

CIS Controls:

Version 6

16.13 User/Account Authentication Must Be Performed Over Encrypted Channels
Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.

Version 7

14.4 Encrypt All Sensitive Information in Transit
Encrypt all sensitive information in transit.

16.5 Encrypt Transmittal of Username and Authentication Credentials
Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.

18.9.97.2.4 (L1) Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WinRM\Service:DisableR
unAs
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Remote Management (WinRM)\WinRM Service\Disallow WinRM
from storing RunAs credentials
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsRemoteManagement.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Impact:

The WinRM service will not allow the `RunAsUser` or `RunAsPassword` configuration values to be set for any plug-ins. If a plug-in has already set the `RunAsUser` and `RunAsPassword` configuration values, the `RunAsPassword` configuration value will be erased from the credential store on the computer.

If this setting is later Disabled again, any values that were previously configured for `RunAsPassword` will need to be reset.

Default Value:

Disabled. (The WinRM service will allow the `RunAsUser` and `RunAsPassword` configuration values to be set for plug-ins and the `RunAsPassword` value will be stored securely.)

References:

1. CCE-36000-8

CIS Controls:

Version 6

16.4 Automatically Log Off Users After Standard Period Of Inactivity
Regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.

Version 7

14.3 Disable Workstation to Workstation Communication
Disable all workstation to workstation communication to limit an attacker's ability to move laterally and compromise neighboring systems, through technologies such as Private VLANs or microsegmentation.

18.9.98 Windows Remote Shell

This section contains settings related to Windows Remote Shell (WinRS).

This Group Policy section is provided by the Group Policy template `WindowsRemoteShell.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.98.1 (L2) Ensure 'Allow Remote Shell Access' is set to 'Disabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy object is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WinRM\Service\WinRS:Al
lowRemoteShellAccess
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Administrative Templates\Windows Components\Windows
Remote Shell\Allow Remote Shell Access
```

Note: This Group Policy path is provided by the Group Policy template `WindowsRemoteShell.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Impact:

New Remote Shell connections are not allowed and are rejected by the server.

Note: On Server 2012 (non-R2) and 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.

Default Value:

Enabled. (New Remote Shell connections are allowed.)

References:

1. CCE-36499-2

CIS Controls:

Version 6

3.4 Use Only Secure Channels For Remote System Administration
Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.

Version 7

4.5 Use Multifactor Authentication For All Administrative Access
Use multi-factor authentication and encrypted channels for all administrative account access.

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

9.3 Perform Regular Automated Port Scans
Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.

18.9.99 Windows Security (formerly Windows Defender 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 `WindowsDefenderSecurityCenter.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Note: This section was originally named *Windows Defender Security Center* but was renamed by Microsoft to *Windows Security* starting with the Microsoft Windows 10 Release 1809 & Server 2019 Administrative Templates.

18.9.100 Windows SideShow

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `SideShow.admx/adml` that is only included with the Microsoft Windows Vista Administrative Templates through Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

18.9.101 Windows System Resource Manager

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `SystemResourceManager.admx/adml` that is only included with the Microsoft Windows Vista through Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

18.9.102 Windows Update

This section contains recommendations related to Windows Update.

This Group Policy section is provided by the Group Policy template `WindowsUpdate.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.102.1 (L1) Ensure 'Configure Automatic Updates' is set to 'Enabled' (Scored)

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 3rd-party solution for patching may choose to exempt themselves from this recommendation, and instead configure it to `Disabled` so that the native Windows Update mechanism does not interfere with the 3rd-party patching process.

Rationale:

Although each version of Windows is thoroughly tested before release, it is possible that problems will be discovered after the products are shipped. The Configure Automatic Updates setting can help you ensure that the computers in your environment will always have the most recent critical operating system updates and service packs installed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU:NoAut
oUpdate
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Update\Configure Automatic Updates
```

Note: This Group Policy path is provided by the Group Policy template `WindowsUpdate.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Impact:

Critical operating system updates and service packs will be installed as necessary.

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.)

References:

1. CCE-36172-5

CIS Controls:

Version 6

4.5 Use Automated Patch Management And Software Update Tools

Deploy automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools are available and safe. Patches should be applied to all systems, even systems that are properly air gapped.

Version 7

3.4 Deploy Automated Operating System Patch Management Tools

Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.

3.5 Deploy Automated Software Patch Management Tools

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.

18.9.102.2 (L1) Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day' (Scored)

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 Rule 18.9.102.2. It will have no impact if any other option is selected.

Rationale:

Although each version of Windows is thoroughly tested before release, it is possible that problems will be discovered after the products are shipped. The Configure Automatic Updates setting can help you ensure that the computers in your environment will always have the most recent critical operating system updates and service packs installed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU:Sched
uledInstallDay
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `0 - Every day`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Update\Configure Automatic Updates: Scheduled install day
```

Note: This Group Policy path is provided by the Group Policy template `WindowsUpdate.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Impact:

If `4 - Auto download and schedule the install` is selected in Rule 18.9.102.2, critical operating system updates and service packs will automatically download every day (at 3:00 A.M., by default).

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.)

References:

1. CCE-36172-5

CIS Controls:

Version 6

4.5 Use Automated Patch Management And Software Update Tools
Deploy automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools are available and safe. Patches should be applied to all systems, even systems that are properly air gapped.

Version 7

3.4 Deploy Automated Operating System Patch Management Tools
Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.

3.5 Deploy Automated Software Patch Management Tools
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.

18.9.102.3 (L1) Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU:NoAut
oRebootWithLoggedOnUsers
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Update\No auto-restart with logged on users for scheduled
automatic updates installations
```

Note: This Group Policy path is provided by the Group Policy template `WindowsUpdate.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.
Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *No auto-restart for scheduled Automatic Updates installations*, but it was renamed starting with the Windows 7 & Server 2008 R2 Administrative Templates.

Impact:

None - this is the default behavior.

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.)

References:

1. CCE-37027-0

CIS Controls:

Version 6

4.5 Use Automated Patch Management And Software Update Tools

Deploy automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools are available and safe. Patches should be applied to all systems, even systems that are properly air gapped.

Version 7

3.4 Deploy Automated Operating System Patch Management Tools

Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.

3.5 Deploy Automated Software Patch Management Tools

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).

19.1 Control Panel

This section contains recommendations for Control Panel settings.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.1.1 Add or Remove Programs

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `AddRemovePrograms.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.1.2 Display

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `ControlPanelDisplay.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.1.3 Personalization (formerly Desktop Themes)

This section contains recommendations for personalization settings.

This Group Policy section is provided by the Group Policy template `ControlPanelDisplay.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note: This section was initially named *Desktop Themes* but was renamed by Microsoft to *Personalization* starting with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates.

19.1.3.1 (L1) Ensure 'Enable screen saver' is set to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting enables/disables the use of desktop screen savers.

The recommended state for this setting is: `Enabled`.

Rationale:

If a user forgets to lock their computer when they walk away, it is possible that a passerby will hijack it. Configuring a timed screen saver with password lock will help to protect against these hijacks.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\[USER SID]\Software\Policies\Microsoft\Windows\Control
Panel\Desktop:ScreenSaveActive
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
User Configuration\Policies\Administrative Templates\Control
Panel\Personalization\Enable screen saver
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `ControlPanelDisplay.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Impact:

A screen saver runs, provided that the following two conditions hold: First, a valid screen saver on the client is specified through the *Force specific screen saver* setting (Rule 19.1.3.2) or through Control Panel on the client computer. Second, the *Screen saver timeout* setting (Rule 19.1.3.4) is set to a nonzero value through the setting or through Control Panel.

Default Value:

Enabling/disabling the screen saver is managed locally by the user.

References:

1. CCE-37970-1

CIS Controls:

Version 6

16.5 Ensure Workstation Screen Locks Are Configured
Configure screen locks on systems to limit access to unattended workstations.

Version 7

16.11 Lock Workstation Sessions After Inactivity
Automatically lock workstation sessions after a standard period of inactivity.

19.1.3.2 (L1) Ensure 'Force specific screen saver: Screen saver executable name' is set to 'Enabled: scrnsave.scr' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting specifies the screen saver for the user's desktop.

The recommended state for this setting is: `Enabled: scrnsave.scr`.

Note: If the specified screen saver is not installed on a computer to which this setting applies, the setting is ignored.

Rationale:

If a user forgets to lock their computer when they walk away, it is possible that a passerby will hijack it. Configuring a timed screen saver with password lock will help to protect against these hijacks.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\[USER SID]\Software\Policies\Microsoft\Windows\Control
Panel\Desktop:SCRNSAVE.EXE
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: scrnsave.scr`:

```
User Configuration\Policies\Administrative Templates\Control
Panel\Personalization\Force specific screen saver
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `ControlPanelDisplay.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Impact:

The system displays the specified screen saver on the user's desktop. The drop-down list of screen savers in the Screen Saver dialog in the Personalization or Display Control Panel will be disabled, preventing users from changing the screen saver.

Default Value:

Disabled. (Users can select any screen saver.)

References:

1. CCE-37907-3

CIS Controls:

Version 6

16.5 Ensure Workstation Screen Locks Are Configured
Configure screen locks on systems to limit access to unattended workstations.

Version 7

16.11 Lock Workstation Sessions After Inactivity
Automatically lock workstation sessions after a standard period of inactivity.

19.1.3.3 (L1) Ensure 'Password protect the screen saver' is set to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This setting determines whether screen savers used on the computer are password protected.

The recommended state for this setting is: `Enabled`.

Rationale:

If a user forgets to lock their computer when they walk away, it is possible that a passerby will hijack it. Configuring a timed screen saver with password lock will help to protect against these hijacks.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\[USER SID]\Software\Policies\Microsoft\Windows\Control
Panel\Desktop:ScreenSaverIsSecure
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
User Configuration\Policies\Administrative Templates\Control
Panel\Personalization\Password protect the screen saver
```

Note: This Group Policy path is provided by the Group Policy template `ControlPanelDisplay.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Impact:

All screen savers are password protected. The "Password protected" checkbox on the Screen Saver dialog in the Personalization or Display Control Panel will be disabled, preventing users from changing the password protection setting.

Default Value:

Whether or not to password protect each screen saver is managed locally by the user.

References:

1. CCE-37658-2

CIS Controls:

Version 6

16.5 Ensure Workstation Screen Locks Are Configured
Configure screen locks on systems to limit access to unattended workstations.

Version 7

16.11 Lock Workstation Sessions After Inactivity
Automatically lock workstation sessions after a standard period of inactivity.

19.1.3.4 (L1) Ensure 'Screen saver timeout' is set to 'Enabled: 900 seconds or fewer, but not 0' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This setting specifies how much user idle time must elapse before the screen saver is launched.

The recommended state for this setting is: `Enabled: 900 seconds or fewer, but not 0.`

Note: This setting has no effect under the following circumstances:

- The wait time is set to zero.
- The "Enable Screen Saver" setting is disabled.
- A valid screen existing saver is not selected manually or via the "Screen saver executable name" setting

Rationale:

If a user forgets to lock their computer when they walk away, it is possible that a passerby will hijack it. Configuring a timed screen saver with password lock will help to protect against these hijacks.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\[USER SID]\Software\Policies\Microsoft\Windows\Control
Panel\Desktop:ScreenSaveTimeOut
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 900 or fewer, but not 0`:

```
User Configuration\Policies\Administrative Templates\Control
Panel\Personalization\Screen saver timeout
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `ControlPanelDisplay.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Impact:

The screen saver will automatically activate when the computer has been left unattended for the amount of time specified, and the users will not be able to change the timeout value.

Default Value:

15 minutes. (May subsequently be reconfigured locally by the user.)

References:

1. CCE-37908-1

CIS Controls:

Version 6

16.5 Ensure Workstation Screen Locks Are Configured
Configure screen locks on systems to limit access to unattended workstations.

Version 7

16.11 Lock Workstation Sessions After Inactivity
Automatically lock workstation sessions after a standard period of inactivity.

19.2 Desktop

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.3 Network

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.4 Shared Folders

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `SharedFolders.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.5 Start Menu and Taskbar

This section contains recommendations for Start Menu and Taskbar settings.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.5.1 Notifications

This section contains recommendations for Notification settings.

This Group Policy section is provided by the Group Policy template `WPN.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

19.5.1.1 (L1) Ensure 'Turn off toast notifications on the lock screen' is set to 'Enabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\[USER
SID]\Software\Policies\Microsoft\Windows\CurrentVersion\PushNotifications:NoT
oastApplicationNotificationOnLockScreen
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
User Configuration\Policies\Administrative Templates\Start Menu and
Taskbar\Notifications\Turn off toast notifications on the lock screen
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WPN.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Impact:

Applications will not be able to raise toast notifications on the lock screen.

Default Value:

Disabled. (Toast notifications on the lock screen are enabled and can be turned off by the administrator or user.)

References:

1. CCE-36332-5

CIS Controls:

Version 6

16.5 Ensure Workstation Screen Locks Are Configured
Configure screen locks on systems to limit access to unattended workstations.

Version 7

16.11 Lock Workstation Sessions After Inactivity
Automatically lock workstation sessions after a standard period of inactivity.

19.6 System

This section contains recommendations for System settings.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.6.1 Ctrl+Alt+Del Options

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `CtrlAltDel.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.6.2 Display

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Display.admx/adml` that is included with the Microsoft Windows 10 Release 1803 Administrative Templates (or newer).

19.6.3 Driver Installation

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `DeviceInstallation.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.6.4 Folder Redirection

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `FolderRedirection.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.6.5 Group Policy

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `GroupPolicy.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.6.6 Internet Communication Management

This section contains recommendations related to Internet Communication Management.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.6.6.1 Internet Communication settings

This section contains recommendations related to Internet Communication settings.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.6.6.1.1 (L2) Ensure 'Turn off Help Experience Improvement Program' is set to 'Enabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\[USER
SID]\Software\Policies\Microsoft\Assistance\Client\1.0:NoImplicitFeedback
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
User Configuration\Policies\Administrative Templates\System\Internet
Communication Management\Internet Communication Settings\Turn off Help
Experience Improvement Program
```

Note: This Group Policy path is provided by the Group Policy template `HelpAndSupport.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Impact:

Users cannot participate in the Help Experience Improvement program.

Default Value:

Disabled. (Users can turn on the Help Experience Improvement program feature from the Help and Support settings page.)

References:

1. CCE-37542-8

CIS Controls:

Version 6

13 Data Protection
Data Protection

Version 7

13.3 Monitor and Block Unauthorized Network Traffic
Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.

19.7 Windows Components

This section contains recommendations for Windows Component settings.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.1 Add features to Windows 8 / 8.1 / 10 (formerly Windows Anytime Upgrade)

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsAnytimeUpgrade.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Note: This section was initially named *Windows Anytime Upgrade* but was renamed by Microsoft to *Add features to Windows x* starting with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

19.7.2 App runtime

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `AppXRuntime.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

19.7.3 Application Compatibility

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `AppCompat.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.4 Attachment Manager

This section contains recommendations related to Attachment Manager.

This Group Policy section is provided by the Group Policy template `AttachmentManager.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.4.1 (L1) Ensure 'Do not preserve zone information in file attachments' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\[USER
SID]\Software\Microsoft\Windows\CurrentVersion\Policies\Attachments: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.

Impact:

None - this is the default behavior.

Default Value:

Disabled. (Windows marks file attachments with their zone information.)

References:

1. CCE-37424-9

CIS Controls:

Version 6

7 Email and Web Browser Protections
Email and Web Browser Protections

Version 7

7.1 Ensure Use of Only Fully Supported Browsers and Email Clients
Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor.

19.7.4.2 (L1) Ensure 'Notify antivirus programs when opening attachments' is set to 'Enabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\[USER
SID]\Software\Microsoft\Windows\CurrentVersion\Policies\Attachments:ScanWithA
ntiVirus
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
User Configuration\Policies\Administrative Templates\Windows
Components\Attachment Manager\Notify antivirus programs when opening
attachments
```

Note: This Group Policy path is provided by the Group Policy template `AttachmentManager.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

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.

Default Value:

Disabled. (Windows does not call the registered antivirus program(s) when file attachments are opened.)

References:

1. CCE-36622-9

CIS Controls:

Version 6

7.8 Scan All Inbound E-mail Attachments For Malicious Code
Scan and block all e-mail attachments entering the organization's e-mail gateway if they contain malicious code or file types that are unnecessary for the organization's business. This scanning should be done before the e-mail is placed in the user's inbox. This includes e-mail content filtering and web content filtering.

Version 7

7.10 Sandbox All Email Attachments
Use sandboxing to analyze and block inbound email attachments with malicious behavior.

7.9 Block Unnecessary File Types
Block all e-mail attachments entering the organization's e-mail gateway if the file types are unnecessary for the organization's business.

8.1 Utilize Centrally Managed Anti-malware Software
Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.

8.2 Ensure Anti-Malware Software and Signatures are Updated
Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.

19.7.5 AutoPlay Policies

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `AutoPlay.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.6 Backup

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `UserDataBackup.admx/adml` that is included only with the Microsoft Windows Vista through Windows 8.0 & Server 2012 (non-R2) Administrative Templates, as well as the Microsoft Windows 10 RTM (Release 1507) and Windows 10 Release 1511 Administrative Templates.

19.7.7 Cloud Content

This section is 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 1607 & Server 2016 Administrative Templates (or newer).

19.7.8 Credential User Interface

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `CredUI.admx/adml` that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

19.7.9 Data Collection and Preview Builds

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `DataCollection.admx/adml` that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

19.7.10 Desktop Gadgets

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Sidebar.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

19.7.11 Desktop Window Manager

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `DWM.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.12 Digital Locker

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `DigitalLocker.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.13 Edge UI

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `EdgeUI.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

19.7.14 File Explorer (formerly Windows Explorer)

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note: This section was initially named *Windows Explorer* but was renamed by Microsoft to *File Explorer* starting with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

19.7.15 File Revocation

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `FileRevocation.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

19.7.16 IME

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `EAIME.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

19.7.17 Import Video

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `CaptureWizard.admx/adml` that is only included with the Microsoft Windows Vista and Windows Server 2008 (non-R2) Administrative Templates.

19.7.18 Instant Search

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WordWheel.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.19 Internet Explorer

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `InetRes.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.20 Location and Sensors

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Sensors.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

19.7.21 Microsoft Edge

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `MicrosoftEdge.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

19.7.22 Microsoft Management Console

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `MMC.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.23 Microsoft User Experience Virtualization

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `UserExperienceVirtualization.admx/adml` that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

19.7.24 NetMeeting

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Conf.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.25 Network Projector

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `NetworkProjection.admx/adml` that is only included with the Microsoft Windows Vista through the Windows 8.1 Update & Server 2012 R2 Update Administrative Templates.

19.7.26 Network Sharing

This section contains recommendations related to Network Sharing.

This Group Policy section is provided by the Group Policy template `Sharing.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.26.1 (L1) Ensure 'Prevent users from sharing files within their profile.' is set to 'Enabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\[USER
SID]\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer:NoInplaceSha
ring
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
User Configuration\Policies\Administrative Templates\Windows
Components\Network Sharing\Prevent users from sharing files within their
profile.
```

Note: This Group Policy path is provided by the Group Policy template `Sharing.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

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.

Default Value:

Disabled. (Users can share files out of their user profile after an administrator has opted in the computer.)

References:

1. CCE-38070-9

CIS Controls:

Version 6

14.4 Protect Information With Access Control Lists
All information stored on systems shall be protected 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.

Version 7

14.6 Protect Information through Access Control Lists
Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

19.7.27 OOBE

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `OOBE.admx/adml` that is included with the Microsoft Windows 10 Release 1809 and Server 2019 Administrative Templates (or newer).

19.7.28 Presentation Settings

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `MobilePCPresentationSettings.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.29 Remote Desktop Services (formerly Terminal Services)

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note: This section was initially named *Terminal Services* but was renamed by Microsoft to *Remote Desktop Services* starting with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates.

19.7.30 RSS Feeds

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `InetRes.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.31 Search

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Search.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

19.7.32 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 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).

19.7.39 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.

19.7.40 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.

19.7.41 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.

19.7.41.1 (L1) Ensure 'Always install with elevated privileges' is set to 'Disabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\[USER
SID]\Software\Policies\Microsoft\Windows\Installer:AlwaysInstallElevated
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
User Configuration\Policies\Administrative Templates\Windows
Components\Windows Installer\Always install with elevated privileges
```

Note: This Group Policy path is provided by the Group Policy template `MSI.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Impact:

None - this is the default behavior.

Default Value:

Disabled. (Windows Installer will apply the current user's permissions when it installs programs that a system administrator does not distribute or offer. This will prevent standard users from installing applications that affect system-wide configuration items.)

References:

1. CCE-37490-0

CIS Controls:

Version 6

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Version 7

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.

4.6 Use of Dedicated Machines For All Administrative Tasks
Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.

19.7.42 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.

19.7.43 Windows Mail

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsMail.admx/adml` that is only included with the Microsoft Windows Vista through the Windows 10 Release 1703 Administrative Templates.

19.7.44 Windows Media Center

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `MediaCenter.admx/adml` that is only included with the Microsoft Windows Vista through Windows 10 Release 1511 Administrative Templates.

19.7.45 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.

19.7.45.1 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.

19.7.45.2 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.

19.7.45.2.1 (L2) Ensure 'Prevent Codec Download' is set to 'Enabled' (Scored)

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\[USER
SID]\Software\Policies\Microsoft\WindowsMediaPlayer:PreventCodecDownload
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
User Configuration\Policies\Administrative Templates\Windows
Components\Windows Media Player\Playback\Prevent Codec Download
```

Note: This Group Policy path is provided by the Group Policy template `WindowsMediaPlayer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

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.

Default Value:

Users can change the setting for the *Download codecs automatically* check box.

References:

1. CCE-37445-4

CIS Controls:

Version 6

2 Inventory of Authorized and Unauthorized Software
Inventory of Authorized and Unauthorized Software

Version 7

2.3 Utilize Software Inventory Tools
Utilize software inventory tools throughout the organization to automate the documentation of all software on business systems.

2.6 Address unapproved software
Ensure that unauthorized software is either removed or the inventory is updated in a timely manner

Appendix: Summary Table

Control		Set Correctly	
		Yes	No
1	**Account Policies**		
1.1	**Password Policy**		
1.1.1	(L1) Ensure 'Enforce password history' is set to '24 or more password(s)' (Scored)	☐	☐
1.1.2	(L1) Ensure 'Maximum password age' is set to '60 or fewer days, but not 0' (Scored)	☐	☐
1.1.3	(L1) Ensure 'Minimum password age' is set to '1 or more day(s)' (Scored)	☐	☐
1.1.4	(L1) Ensure 'Minimum password length' is set to '14 or more character(s)' (Scored)	☐	☐
1.1.5	(L1) Ensure 'Password must meet complexity requirements' is set to 'Enabled' (Scored)	☐	☐
1.1.6	(L1) Ensure 'Store passwords using reversible encryption' is set to 'Disabled' (Scored)	☐	☐
1.2	**Account Lockout Policy**		
1.2.1	(L1) Ensure 'Account lockout duration' is set to '15 or more minute(s)' (Scored)	☐	☐
1.2.2	(L1) Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0' (Scored)	☐	☐
1.2.3	(L1) Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)' (Scored)	☐	☐
2	**Local Policies**		
2.1	**Audit Policy**		
2.2	**User Rights Assignment**		
2.2.1	(L1) Ensure 'Access Credential Manager as a trusted caller' is set to 'No One' (Scored)	☐	☐
2.2.2	(L1) Ensure 'Access this computer from the network' is set to 'Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS' (DC only) (Scored)	☐	☐
2.2.3	(L1) Ensure 'Access this computer from the network' is set to 'Administrators, Authenticated Users' (MS only) (Scored)	☐	☐
2.2.4	(L1) Ensure 'Act as part of the operating system' is set to 'No One' (Scored)	☐	☐
2.2.5	(L1) Ensure 'Add workstations to domain' is set to 'Administrators' (DC only) (Scored)	☐	☐
2.2.6	(L1) Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE' (Scored)	☐	☐

Control		Set Correctly	
		Yes	No
2.2.7	(L1) Ensure 'Allow log on locally' is set to 'Administrators' (Scored)	☐	☐
2.2.8	(L1) Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators' (DC only) (Scored)	☐	☐
2.2.9	(L1) Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators, Remote Desktop Users' (MS only) (Scored)	☐	☐
2.2.10	(L1) Ensure 'Back up files and directories' is set to 'Administrators' (Scored)	☐	☐
2.2.11	(L1) Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE' (Scored)	☐	☐
2.2.12	(L1) Ensure 'Change the time zone' is set to 'Administrators, LOCAL SERVICE' (Scored)	☐	☐
2.2.13	(L1) Ensure 'Create a pagefile' is set to 'Administrators' (Scored)	☐	☐
2.2.14	(L1) Ensure 'Create a token object' is set to 'No One' (Scored)	☐	☐
2.2.15	(L1) Ensure 'Create global objects' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (Scored)	☐	☐
2.2.16	(L1) Ensure 'Create permanent shared objects' is set to 'No One' (Scored)	☐	☐
2.2.17	(L1) Ensure 'Create symbolic links' is set to 'Administrators' (DC only) (Scored)	☐	☐
2.2.18	(L1) Ensure 'Create symbolic links' is set to 'Administrators, NT VIRTUAL MACHINE\Virtual Machines' (MS only) (Scored)	☐	☐
2.2.19	(L1) Ensure 'Debug programs' is set to 'Administrators' (Scored)	☐	☐
2.2.20	(L1) Ensure 'Deny access to this computer from the network' to include 'Guests' (DC only) (Scored)	☐	☐
2.2.21	(L1) Ensure 'Deny access to this computer from the network' to include 'Guests, Local account and member of Administrators group' (MS only) (Scored)	☐	☐
2.2.22	(L1) Ensure 'Deny log on as a batch job' to include 'Guests' (Scored)	☐	☐
2.2.23	(L1) Ensure 'Deny log on as a service' to include 'Guests' (Scored)	☐	☐
2.2.24	(L1) Ensure 'Deny log on locally' to include 'Guests' (Scored)	☐	☐
2.2.25	(L1) Ensure 'Deny log on through Remote Desktop Services' to include 'Guests' (DC only) (Scored)	☐	☐

Control		Set Correctly	
		Yes	No
2.2.26	(L1) Ensure 'Deny log on through Remote Desktop Services' is set to 'Guests, Local account' (MS only) (Scored)	☐	☐
2.2.27	(L1) Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'Administrators' (DC only) (Scored)	☐	☐
2.2.28	(L1) Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'No One' (MS only) (Scored)	☐	☐
2.2.29	(L1) Ensure 'Force shutdown from a remote system' is set to 'Administrators' (Scored)	☐	☐
2.2.30	(L1) Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE' (Scored)	☐	☐
2.2.31	(L1) Ensure 'Impersonate a client after authentication' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (DC only) (Scored)	☐	☐
2.2.32	(L1) 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) (Scored)	☐	☐
2.2.33	(L1) Ensure 'Increase scheduling priority' is set to 'Administrators' (Scored)	☐	☐
2.2.34	(L1) Ensure 'Load and unload device drivers' is set to 'Administrators' (Scored)	☐	☐
2.2.35	(L1) Ensure 'Lock pages in memory' is set to 'No One' (Scored)	☐	☐
2.2.36	(L2) Ensure 'Log on as a batch job' is set to 'Administrators' (DC Only) (Scored)	☐	☐
2.2.37	(L1) Ensure 'Manage auditing and security log' is set to 'Administrators' and (when Exchange is running in the environment) 'Exchange Servers' (DC only) (Scored)	☐	☐
2.2.38	(L1) Ensure 'Manage auditing and security log' is set to 'Administrators' (MS only) (Scored)	☐	☐
2.2.39	(L1) Ensure 'Modify an object label' is set to 'No One' (Scored)	☐	☐
2.2.40	(L1) Ensure 'Modify firmware environment values' is set to 'Administrators' (Scored)	☐	☐
2.2.41	(L1) Ensure 'Perform volume maintenance tasks' is set to 'Administrators' (Scored)	☐	☐
2.2.42	(L1) Ensure 'Profile single process' is set to 'Administrators' (Scored)	☐	☐

Control		Set Correctly	
		Yes	No
2.2.43	(L1) Ensure 'Profile system performance' is set to 'Administrators, NT SERVICE\WdiServiceHost' (Scored)	☐	☐
2.2.44	(L1) Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE' (Scored)	☐	☐
2.2.45	(L1) Ensure 'Restore files and directories' is set to 'Administrators' (Scored)	☐	☐
2.2.46	(L1) Ensure 'Shut down the system' is set to 'Administrators' (Scored)	☐	☐
2.2.47	(L1) Ensure 'Synchronize directory service data' is set to 'No One' (DC only) (Scored)	☐	☐
2.2.48	(L1) Ensure 'Take ownership of files or other objects' is set to 'Administrators' (Scored)	☐	☐
2.3	**Security Options**		
2.3.1	**Accounts**		
2.3.1.1	(L1) Ensure 'Accounts: Administrator account status' is set to 'Disabled' (MS only) (Scored)	☐	☐
2.3.1.2	(L1) Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts' (Scored)	☐	☐
2.3.1.3	(L1) Ensure 'Accounts: Guest account status' is set to 'Disabled' (MS only) (Scored)	☐	☐
2.3.1.4	(L1) Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled' (Scored)	☐	☐
2.3.1.5	(L1) Configure 'Accounts: Rename administrator account' (Scored)	☐	☐
2.3.1.6	(L1) Configure 'Accounts: Rename guest account' (Scored)	☐	☐
2.3.2	**Audit**		
2.3.2.1	(L1) Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled' (Scored)	☐	☐
2.3.2.2	(L1) Ensure 'Audit: Shut down system immediately if unable to log security audits' is set to 'Disabled' (Scored)	☐	☐
2.3.3	**DCOM**		
2.3.4	**Devices**		
2.3.4.1	(L1) Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators' (Scored)	☐	☐
2.3.4.2	(L1) Ensure 'Devices: Prevent users from installing printer drivers' is set to 'Enabled' (Scored)	☐	☐
2.3.5	**Domain controller**		
2.3.5.1	(L1) Ensure 'Domain controller: Allow server operators to schedule tasks' is set to 'Disabled' (DC only) (Scored)	☐	☐

Control		Set Correctly	
		Yes	No
2.3.5.2	(L1) Ensure 'Domain controller: LDAP server signing requirements' is set to 'Require signing' (DC only) (Scored)	☐	☐
2.3.5.3	(L1) Ensure 'Domain controller: Refuse machine account password changes' is set to 'Disabled' (DC only) (Scored)	☐	☐
2.3.6	**Domain member**		
2.3.6.1	(L1) Ensure 'Domain member: Digitally encrypt or sign secure channel data (always)' is set to 'Enabled' (Scored)	☐	☐
2.3.6.2	(L1) Ensure 'Domain member: Digitally encrypt secure channel data (when possible)' is set to 'Enabled' (Scored)	☐	☐
2.3.6.3	(L1) Ensure 'Domain member: Digitally sign secure channel data (when possible)' is set to 'Enabled' (Scored)	☐	☐
2.3.6.4	(L1) Ensure 'Domain member: Disable machine account password changes' is set to 'Disabled' (Scored)	☐	☐
2.3.6.5	(L1) Ensure 'Domain member: Maximum machine account password age' is set to '30 or fewer days, but not 0' (Scored)	☐	☐
2.3.6.6	(L1) Ensure 'Domain member: Require strong (Windows 2000 or later) session key' is set to 'Enabled' (Scored)	☐	☐
2.3.7	**Interactive logon**		
2.3.7.1	(L1) Ensure 'Interactive logon: Do not display last user name' is set to 'Enabled' (Scored)	☐	☐
2.3.7.2	(L1) Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled' (Scored)	☐	☐
2.3.7.3	(L1) Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0' (Scored)	☐	☐
2.3.7.4	(L1) Configure 'Interactive logon: Message text for users attempting to log on' (Scored)	☐	☐
2.3.7.5	(L1) Configure 'Interactive logon: Message title for users attempting to log on' (Scored)	☐	☐
2.3.7.6	(L2) Ensure 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' is set to '4 or fewer logon(s)' (MS only) (Scored)	☐	☐
2.3.7.7	(L1) Ensure 'Interactive logon: Prompt user to change password before expiration' is set to 'between 5 and 14 days' (Scored)	☐	☐
2.3.7.8	(L1) Ensure 'Interactive logon: Require Domain Controller Authentication to unlock workstation' is set to 'Enabled' (MS only) (Scored)	☐	☐
2.3.7.9	(L1) Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher (Scored)	☐	☐
2.3.8	**Microsoft network client**		

Control		Set Correctly	
		Yes	No
2.3.8.1	(L1) Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled' (Scored)	☐	☐
2.3.8.2	(L1) Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled' (Scored)	☐	☐
2.3.8.3	(L1) Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled' (Scored)	☐	☐
2.3.9	**Microsoft network server**		
2.3.9.1	(L1) Ensure 'Microsoft network server: Amount of idle time required before suspending session' is set to '15 or fewer minute(s)' (Scored)	☐	☐
2.3.9.2	(L1) Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled' (Scored)	☐	☐
2.3.9.3	(L1) Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled' (Scored)	☐	☐
2.3.9.4	(L1) Ensure 'Microsoft network server: Disconnect clients when logon hours expire' is set to 'Enabled' (Scored)	☐	☐
2.3.9.5	(L1) Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher (MS only) (Scored)	☐	☐
2.3.10	**Network access**		
2.3.10.1	(L1) Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled' (Scored)	☐	☐
2.3.10.2	(L1) Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled' (MS only) (Scored)	☐	☐
2.3.10.3	(L1) Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled' (MS only) (Scored)	☐	☐
2.3.10.4	(L2) Ensure 'Network access: Do not allow storage of passwords and credentials for network authentication' is set to 'Enabled' (Scored)	☐	☐
2.3.10.5	(L1) Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled' (Scored)	☐	☐
2.3.10.6	(L1) Configure 'Network access: Named Pipes that can be accessed anonymously' (DC only) (Scored)	☐	☐
2.3.10.7	(L1) Configure 'Network access: Named Pipes that can be accessed anonymously' (MS only) (Scored)	☐	☐

Control		Set Correctly	
		Yes	No
2.3.10.8	(L1) Configure 'Network access: Remotely accessible registry paths' (Scored)	☐	☐
2.3.10.9	(L1) Configure 'Network access: Remotely accessible registry paths and sub-paths' (Scored)	☐	☐
2.3.10.10	(L1) Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled' (Scored)	☐	☐
2.3.10.11	(L1) Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None' (Scored)	☐	☐
2.3.10.12	(L1) Ensure 'Network access: Sharing and security model for local accounts' is set to 'Classic - local users authenticate as themselves' (Scored)	☐	☐
2.3.11	**Network security**		
2.3.11.1	(L1) Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled' (Scored)	☐	☐
2.3.11.2	(L1) Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled' (Scored)	☐	☐
2.3.11.3	(L1) Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled' (Scored)	☐	☐
2.3.11.4	(L1) Ensure 'Network security: Configure encryption types allowed for Kerberos' is set to 'AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types' (Scored)	☐	☐
2.3.11.5	(L1) Ensure 'Network security: Do not store LAN Manager hash value on next password change' is set to 'Enabled' (Scored)	☐	☐
2.3.11.6	(L1) Ensure 'Network security: Force logoff when logon hours expire' is set to 'Enabled' (Not Scored)	☐	☐
2.3.11.7	(L1) Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM' (Scored)	☐	☐
2.3.11.8	(L1) Ensure 'Network security: LDAP client signing requirements' is set to 'Negotiate signing' or higher (Scored)	☐	☐
2.3.11.9	(L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit encryption' (Scored)	☐	☐
2.3.11.10	(L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption' (Scored)	☐	☐
2.3.12	**Recovery console**		

Control		Set Correctly	
		Yes	No
2.3.13	**Shutdown**		
2.3.13.1	(L1) Ensure 'Shutdown: Allow system to be shut down without having to log on' is set to 'Disabled' (Scored)	☐	☐
2.3.14	**System cryptography**		
2.3.15	**System objects**		
2.3.15.1	(L1) Ensure 'System objects: Require case insensitivity for non-Windows subsystems' is set to 'Enabled' (Scored)	☐	☐
2.3.15.2	(L1) Ensure 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)' is set to 'Enabled' (Scored)	☐	☐
2.3.16	**System settings**		
2.3.16.1	(L1) Ensure 'System settings: Optional subsystems' is set to 'Defined: (blank)' (Scored)	☐	☐
2.3.17	**User Account Control**		
2.3.17.1	(L1) Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled' (Scored)	☐	☐
2.3.17.2	(L1) Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop' (Scored)	☐	☐
2.3.17.3	(L1) Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests' (Scored)	☐	☐
2.3.17.4	(L1) Ensure 'User Account Control: Detect application installations and prompt for elevation' is set to 'Enabled' (Scored)	☐	☐
2.3.17.5	(L1) Ensure 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' is set to 'Enabled' (Scored)	☐	☐
2.3.17.6	(L1) Ensure 'User Account Control: Run all administrators in Admin Approval Mode' is set to 'Enabled' (Scored)	☐	☐
2.3.17.7	(L1) Ensure 'User Account Control: Switch to the secure desktop when prompting for elevation' is set to 'Enabled' (Scored)	☐	☐
2.3.17.8	(L1) Ensure 'User Account Control: Virtualize file and registry write failures to per-user locations' is set to 'Enabled' (Scored)	☐	☐
3	**Event Log**		
4	**Restricted Groups**		
5	**System Services**		

Control		Set Correctly	
		Yes	No
6	**Registry**		
7	**File System**		
8	**Wired Network (IEEE 802.3) Policies**		
9	**Windows Firewall with Advanced Security**		
9.1	**Domain Profile**		
9.1.1	(L1) Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)' (Scored)	☐	☐
9.1.2	(L1) Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)' (Scored)	☐	☐
9.1.3	(L1) Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)' (Scored)	☐	☐
9.1.4	(L1) Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No' (Scored)	☐	☐
9.1.5	(L1) Ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\domainfw.log' (Scored)	☐	☐
9.1.6	(L1) Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater' (Scored)	☐	☐
9.1.7	(L1) Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes' (Scored)	☐	☐
9.1.8	(L1) Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes' (Scored)	☐	☐
9.2	**Private Profile**		
9.2.1	(L1) Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)' (Scored)	☐	☐
9.2.2	(L1) Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)' (Scored)	☐	☐
9.2.3	(L1) Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)' (Scored)	☐	☐
9.2.4	(L1) Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No' (Scored)	☐	☐
9.2.5	(L1) Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\privatefw.log' (Scored)	☐	☐
9.2.6	(L1) Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater' (Scored)	☐	☐
9.2.7	(L1) Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes' (Scored)	☐	☐

Control		Set Correctly	
		Yes	No
9.2.8	(L1) Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes' (Scored)	☐	☐
9.3	**Public Profile**		
9.3.1	(L1) Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)' (Scored)	☐	☐
9.3.2	(L1) Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)' (Scored)	☐	☐
9.3.3	(L1) Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)' (Scored)	☐	☐
9.3.4	(L1) Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'No' (Scored)	☐	☐
9.3.5	(L1) Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No' (Scored)	☐	☐
9.3.6	(L1) Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No' (Scored)	☐	☐
9.3.7	(L1) Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\publicfw.log' (Scored)	☐	☐
9.3.8	(L1) Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater' (Scored)	☐	☐
9.3.9	(L1) Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes' (Scored)	☐	☐
9.3.10	(L1) Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes' (Scored)	☐	☐
10	**Network List Manager Policies**		
11	**Wireless Network (IEEE 802.11) Policies**		
12	**Public Key Policies**		
13	**Software Restriction Policies**		
14	**Network Access Protection NAP Client Configuration**		
15	**Application Control Policies**		
16	**IP Security Policies**		
17	**Advanced Audit Policy Configuration**		
17.1	**Account Logon**		
17.1.1	(L1) Ensure 'Audit Credential Validation' is set to 'Success and Failure' (Scored)	☐	☐
17.1.2	(L1) Ensure 'Audit Kerberos Authentication Service' is set to 'Success and Failure' (DC Only) (Scored)	☐	☐
17.1.3	(L1) Ensure 'Audit Kerberos Service Ticket Operations' is set to 'Success and Failure' (DC Only) (Scored)	☐	☐
17.2	**Account Management**		

Control		Set Correctly	
		Yes	No
17.2.1	(L1) Ensure 'Audit Application Group Management' is set to 'Success and Failure' (Scored)	☐	☐
17.2.2	(L1) Ensure 'Audit Computer Account Management' is set to include 'Success' (DC only) (Scored)	☐	☐
17.2.3	(L1) Ensure 'Audit Distribution Group Management' is set to include 'Success' (DC only) (Scored)	☐	☐
17.2.4	(L1) Ensure 'Audit Other Account Management Events' is set to include 'Success' (DC only) (Scored)	☐	☐
17.2.5	(L1) Ensure 'Audit Security Group Management' is set to include 'Success' (Scored)	☐	☐
17.2.6	(L1) Ensure 'Audit User Account Management' is set to 'Success and Failure' (Scored)	☐	☐
17.3	**Detailed Tracking**		
17.3.1	(L1) Ensure 'Audit Process Creation' is set to include 'Success' (Scored)	☐	☐
17.4	**DS Access**		
17.4.1	(L1) Ensure 'Audit Directory Service Access' is set to include 'Failure' (DC only) (Scored)	☐	☐
17.4.2	(L1) Ensure 'Audit Directory Service Changes' is set to include 'Success' (DC only) (Scored)	☐	☐
17.5	**Logon/Logoff**		
17.5.1	(L1) Ensure 'Audit Account Lockout' is set to include 'Failure' (Scored)	☐	☐
17.5.2	(L1) Ensure 'Audit Logoff' is set to include 'Success' (Scored)	☐	☐
17.5.3	(L1) Ensure 'Audit Logon' is set to 'Success and Failure' (Scored)	☐	☐
17.5.4	(L1) Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure' (Scored)	☐	☐
17.5.5	(L1) Ensure 'Audit Special Logon' is set to include 'Success' (Scored)	☐	☐
17.6	**Object Access**		
17.6.1	(L1) Ensure 'Audit Detailed File Share' is set to include 'Failure' (Scored)	☐	☐
17.6.2	(L1) Ensure 'Audit File Share' is set to 'Success and Failure' (Scored)	☐	☐
17.6.3	(L1) Ensure 'Audit Other Object Access Events' is set to 'Success and Failure' (Scored)	☐	☐
17.6.4	(L1) Ensure 'Audit Removable Storage' is set to 'Success and Failure' (Scored)	☐	☐
17.7	**Policy Change**		

Control		Set Correctly	
		Yes	No
17.7.1	(L1) Ensure 'Audit Audit Policy Change' is set to include 'Success' (Scored)	☐	☐
17.7.2	(L1) Ensure 'Audit Authentication Policy Change' is set to include 'Success' (Scored)	☐	☐
17.7.3	(L1) Ensure 'Audit Authorization Policy Change' is set to include 'Success' (Scored)	☐	☐
17.7.4	(L1) Ensure 'Audit MPSSVC Rule-Level Policy Change' is set to 'Success and Failure' (Scored)	☐	☐
17.7.5	(L1) Ensure 'Audit Other Policy Change Events' is set to include 'Failure' (Scored)	☐	☐
17.8	**Privilege Use**		
17.8.1	(L1) Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure' (Scored)	☐	☐
17.9	**System**		
17.9.1	(L1) Ensure 'Audit IPsec Driver' is set to 'Success and Failure' (Scored)	☐	☐
17.9.2	(L1) Ensure 'Audit Other System Events' is set to 'Success and Failure' (Scored)	☐	☐
17.9.3	(L1) Ensure 'Audit Security State Change' is set to include 'Success' (Scored)	☐	☐
17.9.4	(L1) Ensure 'Audit Security System Extension' is set to include 'Success' (Scored)	☐	☐
17.9.5	(L1) Ensure 'Audit System Integrity' is set to 'Success and Failure' (Scored)	☐	☐
18	**Administrative Templates (Computer)**		
18.1	**Control Panel**		
18.2	**LAPS**		
18.2.1	(L1) Ensure LAPS AdmPwd GPO Extension / CSE is installed (MS only) (Scored)	☐	☐
18.2.2	(L1) Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled' (MS only) (Scored)	☐	☐
18.2.3	(L1) Ensure 'Enable Local Admin Password Management' is set to 'Enabled' (MS only) (Scored)	☐	☐
18.2.4	(L1) Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + special characters' (MS only) (Scored)	☐	☐
18.2.5	(L1) Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more' (MS only) (Scored)	☐	☐
18.2.6	(L1) Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer' (MS only) (Scored)	☐	☐

Control		Set Correctly	
		Yes	No
18.3	**MS Security Guide**		
18.3.1	(L1) Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled' (MS only) (Scored)	☐	☐
18.3.2	(L1) Ensure 'Configure SMB v1 client' is set to 'Enabled: Bowser, MRxSmb20, NSI' (Scored)	☐	☐
18.3.3	(L1) Ensure 'Configure SMB v1 client driver' is set to 'Enabled: Disable driver (recommended)' (Scored)	☐	☐
18.3.4	(L1) Ensure 'Configure SMB v1 server' is set to 'Disabled' (Scored)	☐	☐
18.3.5	(L1) Ensure 'Enable Structured Exception Handling Overwrite Protection (SEHOP)' is set to 'Enabled' (Scored)	☐	☐
18.3.6	(L1) Ensure 'Extended Protection for LDAP Authentication (Domain Controllers only)' is set to 'Enabled: Enabled, always (recommended)' (DC Only) (Scored)	☐	☐
18.3.7	(L1) Ensure 'NetBT NodeType configuration' is set to 'Enabled: P-node (recommended)' (Scored)	☐	☐
18.3.8	(L1) Ensure 'WDigest Authentication' is set to 'Disabled' (Scored)	☐	☐
18.4	**MSS (Legacy)**		
18.4.1	(L1) Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled' (Scored)	☐	☐
18.4.2	(L1) Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled' (Scored)	☐	☐
18.4.3	(L1) Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled' (Scored)	☐	☐
18.4.4	(L1) Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled' (Scored)	☐	☐
18.4.5	(L2) Ensure 'MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds' is set to 'Enabled: 300,000 or 5 minutes (recommended)' (Scored)	☐	☐
18.4.6	(L1) Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled' (Scored)	☐	☐
18.4.7	(L2) Ensure 'MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)' is set to 'Disabled' (Scored)	☐	☐

Control		Set Correctly	
		Yes	No
18.4.8	(L1) Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled' (Scored)	☐	☐
18.4.9	(L1) Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)' is set to 'Enabled: 5 or fewer seconds' (Scored)	☐	☐
18.4.10	(L2) Ensure 'MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3' (Scored)	☐	☐
18.4.11	(L2) Ensure 'MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3' (Scored)	☐	☐
18.4.12	(L1) Ensure 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' is set to 'Enabled: 90% or less' (Scored)	☐	☐
18.5	**Network**		
18.5.1	**Background Intelligent Transfer Service (BITS)**		
18.5.2	**BranchCache**		
18.5.3	**DirectAccess Client Experience Settings**		
18.5.4	**DNS Client**		
18.5.4.1	(L1) Ensure 'Turn off multicast name resolution' is set to 'Enabled' (Scored)	☐	☐
18.5.5	**Fonts**		
18.5.6	**Hotspot Authentication**		
18.5.7	**Lanman Server**		
18.5.8	**Lanman Workstation**		
18.5.9	**Link-Layer Topology Discovery**		
18.5.9.1	(L2) Ensure 'Turn on Mapper I/O (LLTDIO) driver' is set to 'Disabled' (Scored)	☐	☐
18.5.9.2	(L2) Ensure 'Turn on Responder (RSPNDR) driver' is set to 'Disabled' (Scored)	☐	☐
18.5.10	**Microsoft Peer-to-Peer Networking Services**		
18.5.10.1	(L2) Ensure 'Turn off Microsoft Peer-to-Peer Networking Services' is set to 'Enabled' (Scored)	☐	☐
18.5.11	**Network Connections**		
18.5.11.2	(L1) Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled' (Scored)	☐	☐
18.5.11.3	(L1) Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled' (Scored)	☐	☐
18.5.12	**Network Connectivity Status Indicator**		

Control		Set Correctly	
		Yes	No
18.5.13	**Network Isolation**		
18.5.14	**Network Provider**		
18.5.14.1	(L1) Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares' (Scored)	☐	☐
18.5.15	**Offline Files**		
18.5.16	**QoS Packet Scheduler**		
18.5.17	**SNMP**		
18.5.18	**SSL Configuration Settings**		
18.5.19	**TCPIP Settings**		
18.5.19.1	**IPv6 Transition Technologies**		
18.5.19.2	**Parameters**		
18.5.19.2.1	(L2) Disable IPv6 (Ensure TCPIP6 Parameter 'DisabledComponents' is set to '0xff (255)') (Scored)	☐	☐
18.5.20	**Windows Connect Now**		
18.5.20.1	(L2) Ensure 'Configuration of wireless settings using Windows Connect Now' is set to 'Disabled' (Scored)	☐	☐
18.5.20.2	(L2) Ensure 'Prohibit access of the Windows Connect Now wizards' is set to 'Enabled' (Scored)	☐	☐
18.5.21	**Windows Connection Manager**		
18.5.21.1	(L1) Ensure 'Minimize the number of simultaneous connections to the Internet or a Windows Domain' is set to 'Enabled: 1 = Minimize simultaneous connections' (Scored)	☐	☐
18.5.21.2	(L2) Ensure 'Prohibit connection to non-domain networks when connected to domain authenticated network' is set to 'Enabled' (MS only) (Scored)	☐	☐
18.6	**Printers**		
18.7	**Start Menu and Taskbar**		
18.7.1	**Notifications**		
18.7.1.1	(L2) Ensure 'Turn off notifications network usage' is set to 'Enabled' (Scored)	☐	☐
18.8	**System**		
18.8.1	**Access-Denied Assistance**		
18.8.2	**App-V**		
18.8.3	**Audit Process Creation**		
18.8.4	**Credentials Delegation**		
18.8.4.1	(L1) Ensure 'Encryption Oracle Remediation' is set to 'Enabled: Force Updated Clients' (Scored)	☐	☐
18.8.5	**Device Guard**		
18.8.6	**Device Health Attestation Service**		

Control		Set Correctly	
		Yes	No
18.8.7	**Device Installation**		
18.8.8	**Device Redirection**		
18.8.9	**Disk NV Cache**		
18.8.10	**Disk Quotas**		
18.8.11	**Display**		
18.8.12	**Distributed COM**		
18.8.13	**Driver Installation**		
18.8.14	**Early Launch Antimalware**		
18.8.14.1	(L1) Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good, unknown and bad but critical' (Scored)	☐	☐
18.8.15	**Enhanced Storage Access**		
18.8.16	**File Classification Infrastructure**		
18.8.17	**File Share Shadow Copy Agent**		
18.8.18	**File Share Shadow Copy Provider**		
18.8.19	**Filesystem (formerly NTFS Filesystem)**		
18.8.20	**Folder Redirection**		
18.8.21	**Group Policy**		
18.8.21.2	(L1) Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE' (Scored)	☐	☐
18.8.21.3	(L1) Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE' (Scored)	☐	☐
18.8.21.4	(L1) Ensure 'Turn off background refresh of Group Policy' is set to 'Disabled' (Scored)	☐	☐
18.8.22	**Internet Communication Management**		
18.8.22.1	**Internet Communication settings**		
18.8.22.1.1	(L1) Ensure 'Turn off downloading of print drivers over HTTP' is set to 'Enabled' (Scored)	☐	☐
18.8.22.1.2	(L2) Ensure 'Turn off handwriting personalization data sharing' is set to 'Enabled' (Scored)	☐	☐
18.8.22.1.3	(L2) Ensure 'Turn off handwriting recognition error reporting' is set to 'Enabled' (Scored)	☐	☐
18.8.22.1.4	(L2) Ensure 'Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com' is set to 'Enabled' (Scored)	☐	☐
18.8.22.1.5	(L1) Ensure 'Turn off Internet download for Web publishing and online ordering wizards' is set to 'Enabled' (Scored)	☐	☐
18.8.22.1.6	(L2) Ensure 'Turn off printing over HTTP' is set to 'Enabled' (Scored)	☐	☐

Control		Set Correctly	
		Yes	No
18.8.22.1.7	(L2) Ensure 'Turn off Registration if URL connection is referring to Microsoft.com' is set to 'Enabled' (Scored)	☐	☐
18.8.22.1.8	(L2) Ensure 'Turn off Search Companion content file updates' is set to 'Enabled' (Scored)	☐	☐
18.8.22.1.9	(L2) Ensure 'Turn off the "Order Prints" picture task' is set to 'Enabled' (Scored)	☐	☐
18.8.22.1.10	(L2) Ensure 'Turn off the "Publish to Web" task for files and folders' is set to 'Enabled' (Scored)	☐	☐
18.8.22.1.11	(L2) Ensure 'Turn off the Windows Messenger Customer Experience Improvement Program' is set to 'Enabled' (Scored)	☐	☐
18.8.22.1.12	(L2) Ensure 'Turn off Windows Customer Experience Improvement Program' is set to 'Enabled' (Scored)	☐	☐
18.8.22.1.13	(L2) Ensure 'Turn off Windows Error Reporting' is set to 'Enabled' (Scored)	☐	☐
18.8.23	**iSCSI**		
18.8.24	**KDC**		
18.8.25	**Kerberos**		
18.8.26	**Kernel DMA Protection**		
18.8.27	**Locale Services**		
18.8.27.1	(L2) Ensure 'Disallow copying of user input methods to the system account for sign-in' is set to 'Enabled' (Scored)	☐	☐
18.8.28	**Logon**		
18.8.28.1	(L1) Ensure 'Do not display network selection UI' is set to 'Enabled' (Scored)	☐	☐
18.8.28.2	(L1) Ensure 'Do not enumerate connected users on domain-joined computers' is set to 'Enabled' (Scored)	☐	☐
18.8.28.3	(L1) Ensure 'Enumerate local users on domain-joined computers' is set to 'Disabled' (MS only) (Scored)	☐	☐
18.8.28.4	(L1) Ensure 'Turn off app notifications on the lock screen' is set to 'Enabled' (Scored)	☐	☐
18.8.28.5	(L1) Ensure 'Turn off picture password sign-in' is set to 'Enabled' (Scored)	☐	☐
18.8.28.6	(L1) Ensure 'Turn on convenience PIN sign-in' is set to 'Disabled' (Scored)	☐	☐
18.8.29	**Mitigation Options**		
18.8.30	**Net Logon**		
18.8.31	**OS Policies**		
18.8.32	**Performance Control Panel**		
18.8.33	**PIN Complexity**		

Control		Set Correctly	
		Yes	No
18.8.34	**Power Management**		
18.8.34.1	**Button Settings**		
18.8.34.2	**Energy Saver Settings**		
18.8.34.3	**Hard Disk Settings**		
18.8.34.4	**Notification Settings**		
18.8.34.5	**Power Throttling Settings**		
18.8.34.6	**Sleep Settings**		
18.8.34.6.1	(L1) Ensure 'Require a password when a computer wakes (on battery)' is set to 'Enabled' (Scored)	☐	☐
18.8.34.6.2	(L1) Ensure 'Require a password when a computer wakes (plugged in)' is set to 'Enabled' (Scored)	☐	☐
18.8.35	**Recovery**		
18.8.36	**Remote Assistance**		
18.8.36.1	(L1) Ensure 'Configure Offer Remote Assistance' is set to 'Disabled' (Scored)	☐	☐
18.8.36.2	(L1) Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled' (Scored)	☐	☐
18.8.37	**Remote Procedure Call**		
18.8.37.1	(L1) Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled' (MS only) (Scored)	☐	☐
18.8.37.2	(L2) Ensure 'Restrict Unauthenticated RPC clients' is set to 'Enabled: Authenticated' (MS only) (Scored)	☐	☐
18.8.38	**Removable Storage Access**		
18.8.39	**Scripts**		
18.8.40	**Server Manager**		
18.8.41	**Service Control Manager Settings**		
18.8.42	**Shutdown**		
18.8.43	**Shutdown Options**		
18.8.44	**Storage Health**		
18.8.45	**Storage Sense**		
18.8.46	**System Restore**		
18.8.47	**Troubleshooting and Diagnostics**		
18.8.47.1	**Application Compatibility Diagnostics**		
18.8.47.2	**Corrupted File Recovery**		
18.8.47.3	**Disk Diagnostic**		
18.8.47.4	**Fault Tolerant Heap**		
18.8.47.5	**Microsoft Support Diagnostic Tool**		
18.8.47.5.1	(L2) Ensure 'Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider' is set to 'Disabled' (Scored)	☐	☐

Control		Set Correctly	
		Yes	No
18.8.47.6	**MSI Corrupted File Recovery**		
18.8.47.7	**Scheduled Maintenance**		
18.8.47.8	**Scripted Diagnostics**		
18.8.47.9	**Windows Boot Performance Diagnostics**		
18.8.47.10	**Windows Memory Leak Diagnosis**		
18.8.47.11	**Windows Performance PerfTrack**		
18.8.47.11.1	(L2) Ensure 'Enable/Disable PerfTrack' is set to 'Disabled' (Scored)	☐	☐
18.8.48	**Trusted Platform Module Services**		
18.8.49	**User Profiles**		
18.8.50	**Windows File Protection**		
18.8.51	**Windows HotStart**		
18.8.52	**Windows Time Service**		
18.8.52.1	**Time Providers**		
18.8.52.1.1	(L2) Ensure 'Enable Windows NTP Client' is set to 'Enabled' (Scored)	☐	☐
18.8.52.1.2	(L2) Ensure 'Enable Windows NTP Server' is set to 'Disabled' (MS only) (Scored)	☐	☐
18.9	**Windows Components**		
18.9.1	**Active Directory Federation Services**		
18.9.2	**ActiveX Installer Service**		
18.9.3	**Add features to Windows 8 / 8.1 / 10 (formerly Windows Anytime Upgrade)**		
18.9.4	**App Package Deployment**		
18.9.5	**App Privacy**		
18.9.6	**App runtime**		
18.9.7	**Application Compatibility**		
18.9.8	**AutoPlay Policies**		
18.9.8.1	(L1) Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled' (Scored)	☐	☐
18.9.8.2	(L1) Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands' (Scored)	☐	☐
18.9.8.3	(L1) Ensure 'Turn off Autoplay' is set to 'Enabled: All drives' (Scored)	☐	☐
18.9.9	**Backup**		
18.9.10	**Biometrics**		
18.9.11	**BitLocker Drive Encryption**		
18.9.12	**Camera**		
18.9.13	**Cloud Content**		
18.9.14	**Connect**		

Control		Set Correctly	
		Yes	No
18.9.15	**Credential User Interface**		
18.9.15.1	(L1) Ensure 'Do not display the password reveal button' is set to 'Enabled' (Scored)	☐	☐
18.9.15.2	(L1) Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled' (Scored)	☐	☐
18.9.16	**Data Collection and Preview Builds**		
18.9.17	**Delivery Optimization**		
18.9.18	**Desktop Gadgets**		
18.9.19	**Desktop Window Manager**		
18.9.20	**Device and Driver Compatibility**		
18.9.21	**Device Registration (formerly Workplace Join)**		
18.9.22	**Digital Locker**		
18.9.23	**Edge UI**		
18.9.24	**EMET**		
18.9.24.1	(L1) Ensure 'EMET 5.52' or higher is installed (Scored)	☐	☐
18.9.24.2	(L1) Ensure 'Default Action and Mitigation Settings' is set to 'Enabled' (plus subsettings) (Scored)	☐	☐
18.9.24.3	(L1) Ensure 'Default Protections for Internet Explorer' is set to 'Enabled' (Scored)	☐	☐
18.9.24.4	(L1) Ensure 'Default Protections for Popular Software' is set to 'Enabled' (Scored)	☐	☐
18.9.24.5	(L1) Ensure 'Default Protections for Recommended Software' is set to 'Enabled' (Scored)	☐	☐
18.9.24.6	(L1) Ensure 'System ASLR' is set to 'Enabled: Application Opt-In' (Scored)	☐	☐
18.9.24.7	(L1) Ensure 'System DEP' is set to 'Enabled: Application Opt-Out' (Scored)	☐	☐
18.9.24.8	(L1) Ensure 'System SEHOP' is set to 'Enabled: Application Opt-Out' (Scored)	☐	☐
18.9.25	**Event Forwarding**		
18.9.26	**Event Log Service**		
18.9.26.1	**Application**		
18.9.26.1.1	(L1) Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Scored)	☐	☐
18.9.26.1.2	(L1) Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Scored)	☐	☐
18.9.26.2	**Security**		

Control		Set Correctly	
		Yes	No
18.9.26.2.1	(L1) Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Scored)	☐	☐
18.9.26.2.2	(L1) Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater' (Scored)	☐	☐
18.9.26.3	**Setup**		
18.9.26.3.1	(L1) Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Scored)	☐	☐
18.9.26.3.2	(L1) Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Scored)	☐	☐
18.9.26.4	**System**		
18.9.26.4.1	(L1) Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Scored)	☐	☐
18.9.26.4.2	(L1) Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Scored)	☐	☐
18.9.27	**Event Logging**		
18.9.28	**Event Viewer**		
18.9.29	**Family Safety (formerly Parental Controls)**		
18.9.30	**File Explorer (formerly Windows Explorer)**		
18.9.30.1	(L1) Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled' (Scored)	☐	☐
18.9.30.2	(L1) Ensure 'Turn off heap termination on corruption' is set to 'Disabled' (Scored)	☐	☐
18.9.30.3	(L1) Ensure 'Turn off shell protocol protected mode' is set to 'Disabled' (Scored)	☐	☐
18.9.31	**File History**		
18.9.32	**Find My Device**		
18.9.33	**Game Explorer**		
18.9.34	**Handwriting**		
18.9.35	**HomeGroup**		
18.9.36	**Import Video**		
18.9.37	**Internet Explorer**		
18.9.38	**Internet Information Services**		
18.9.39	**Location and Sensors**		
18.9.39.1	**Windows Location Provider**		
18.9.39.1.1	(L2) Ensure 'Turn off Windows Location Provider' is set to 'Enabled' (Scored)	☐	☐
18.9.39.2	(L2) Ensure 'Turn off location' is set to 'Enabled' (Scored)	☐	☐

Control		Set Correctly	
		Yes	No
18.9.40	**Maintenance Scheduler**		
18.9.41	**Maps**		
18.9.42	**MDM**		
18.9.43	**Messaging**		
18.9.44	**Microsoft account**		
18.9.45	**Microsoft Edge**		
18.9.46	**Microsoft FIDO Authentication**		
18.9.47	**Microsoft Secondary Authentication Factor**		
18.9.48	**Microsoft User Experience Virtualization**		
18.9.49	**NetMeeting**		
18.9.50	**Network Access Protection**		
18.9.51	**Network Projector**		
18.9.52	**OneDrive (formerly SkyDrive)**		
18.9.52.1	(L1) Ensure 'Prevent the usage of OneDrive for file storage' is set to 'Enabled' (Scored)	☐	☐
18.9.52.2	(L1) Ensure 'Prevent the usage of OneDrive for file storage on Windows 8.1' is set to 'Enabled' (Scored)	☐	☐
18.9.53	**Online Assistance**		
18.9.54	**OOBE**		
18.9.55	**Password Synchronization**		
18.9.56	**Portable Operating System**		
18.9.57	**Presentation Settings**		
18.9.58	**Push To Install**		
18.9.59	**Remote Desktop Services (formerly Terminal Services)**		
18.9.59.1	**RD Licensing (formerly TS Licensing)**		
18.9.59.2	**Remote Desktop Connection Client**		
18.9.59.2.1	**RemoteFX USB Device Redirection**		
18.9.59.2.2	(L1) Ensure 'Do not allow passwords to be saved' is set to 'Enabled' (Scored)	☐	☐
18.9.59.3	**Remote Desktop Session Host (formerly Terminal Server)**		
18.9.59.3.1	**Application Compatibility**		
18.9.59.3.2	**Connections**		
18.9.59.3.2.1	(L2) Ensure 'Restrict Remote Desktop Services users to a single Remote Desktop Services session' is set to 'Enabled' (Scored)	☐	☐
18.9.59.3.3	**Device and Resource Redirection**		
18.9.59.3.3.1	(L2) Ensure 'Do not allow COM port redirection' is set to 'Enabled' (Scored)	☐	☐
18.9.59.3.3.2	(L1) Ensure 'Do not allow drive redirection' is set to 'Enabled' (Scored)	☐	☐

Control		Set Correctly	
		Yes	No
18.9.59.3.3.3	(L2) Ensure 'Do not allow LPT port redirection' is set to 'Enabled' (Scored)	☐	☐
18.9.59.3.3.4	(L2) Ensure 'Do not allow supported Plug and Play device redirection' is set to 'Enabled' (Scored)	☐	☐
18.9.59.3.4	**Licensing**		
18.9.59.3.5	**Printer Redirection**		
18.9.59.3.6	**Profiles**		
18.9.59.3.7	**RD Connection Broker (formerly TS Connection Broker)**		
18.9.59.3.8	**Remote Session Environment**		
18.9.59.3.9	**Security**		
18.9.59.3.9.1	(L1) Ensure 'Always prompt for password upon connection' is set to 'Enabled' (Scored)	☐	☐
18.9.59.3.9.2	(L1) Ensure 'Require secure RPC communication' is set to 'Enabled' (Scored)	☐	☐
18.9.59.3.9.3	(L1) Ensure 'Require use of specific security layer for remote (RDP) connections' is set to 'Enabled: SSL' (Scored)	☐	☐
18.9.59.3.9.4	(L1) Ensure 'Require user authentication for remote connections by using Network Level Authentication' is set to 'Enabled' (Scored)	☐	☐
18.9.59.3.9.5	(L1) Ensure 'Set client connection encryption level' is set to 'Enabled: High Level' (Scored)	☐	☐
18.9.59.3.10	**Session Time Limits**		
18.9.59.3.10.1	(L2) Ensure 'Set time limit for active but idle Remote Desktop Services sessions' is set to 'Enabled: 15 minutes or less' (Scored)	☐	☐
18.9.59.3.10.2	(L2) Ensure 'Set time limit for disconnected sessions' is set to 'Enabled: 1 minute' (Scored)	☐	☐
18.9.59.3.11	**Temporary folders**		
18.9.59.3.11.1	(L1) Ensure 'Do not delete temp folders upon exit' is set to 'Disabled' (Scored)	☐	☐
18.9.59.3.11.2	(L1) Ensure 'Do not use temporary folders per session' is set to 'Disabled' (Scored)	☐	☐
18.9.60	**RSS Feeds**		
18.9.60.1	(L1) Ensure 'Prevent downloading of enclosures' is set to 'Enabled' (Scored)	☐	☐
18.9.61	**Search**		
18.9.61.2	(L1) Ensure 'Allow indexing of encrypted files' is set to 'Disabled' (Scored)	☐	☐
18.9.62	**Security Center**		
18.9.63	**Server for NIS**		

Control		Set Correctly	
		Yes	No
18.9.64	**Shutdown Options**		
18.9.65	**Smart Card**		
18.9.66	**Software Protection Platform**		
18.9.66.1	(L2) Ensure 'Turn off KMS Client Online AVS Validation' is set to 'Enabled' (Scored)	☐	☐
18.9.67	**Sound Recorder**		
18.9.68	**Speech**		
18.9.69	**Store**		
18.9.70	**Sync your settings**		
18.9.71	**Tablet PC**		
18.9.72	**Task Scheduler**		
18.9.73	**Text Input**		
18.9.74	**Windows Calendar**		
18.9.75	**Windows Color System**		
18.9.76	**Windows Customer Experience Improvement Program**		
18.9.77	**Windows Defender Antivirus (formerly Windows Defender)**		
18.9.77.1	**Client Interface**		
18.9.77.2	**Exclusions**		
18.9.77.3	**MAPS**		
18.9.77.3.1	(L1) Ensure 'Configure local setting override for reporting to Microsoft MAPS' is set to 'Disabled' (Scored)	☐	☐
18.9.77.3.2	(L2) Ensure 'Join Microsoft MAPS' is set to 'Disabled' (Scored)	☐	☐
18.9.77.4	**MpEngine**		
18.9.77.5	**Network Inspection System**		
18.9.77.6	**Quarantine**		
18.9.77.7	**Real-time Protection**		
18.9.77.7.1	(L1) Ensure 'Turn on behavior monitoring' is set to 'Enabled' (Scored)	☐	☐
18.9.77.8	**Remediation**		
18.9.77.9	**Reporting**		
18.9.77.9.1	(L2) Ensure 'Configure Watson events' is set to 'Disabled' (Scored)	☐	☐
18.9.77.10	**Scan**		
18.9.77.10.1	(L1) Ensure 'Scan removable drives' is set to 'Enabled' (Scored)	☐	☐
18.9.77.10.2	(L1) Ensure 'Turn on e-mail scanning' is set to 'Enabled' (Scored)	☐	☐
18.9.77.11	**Security Intelligence Updates (formerly Signature Updates)**		
18.9.77.12	**Threats**		

Control		Set Correctly	
		Yes	No
18.9.77.13	**Windows Defender Exploit Guard**		
18.9.77.14	(L1) Ensure 'Turn off Windows Defender AntiVirus' is set to 'Disabled' (Scored)	☐	☐
18.9.78	**Windows Defender Application Guard**		
18.9.79	**Windows Defender Exploit Guard**		
18.9.80	**Windows Defender SmartScreen**		
18.9.80.1	**Explorer**		
18.9.80.1.1	(L1) Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled: Warn and prevent bypass' (Scored)	☐	☐
18.9.81	**Windows Error Reporting**		
18.9.81.1	**Advanced Error Reporting Settings**		
18.9.81.2	**Consent**		
18.9.81.2.1	(L1) Ensure 'Configure Default consent' is set to 'Enabled: Always ask before sending data' (Scored)	☐	☐
18.9.82	**Windows Game Recording and Broadcasting**		
18.9.83	**Windows Hello for Business (formerly Microsoft Passport for Work)**		
18.9.84	**Windows Ink Workspace**		
18.9.85	**Windows Installer**		
18.9.85.1	(L1) Ensure 'Allow user control over installs' is set to 'Disabled' (Scored)	☐	☐
18.9.85.2	(L1) Ensure 'Always install with elevated privileges' is set to 'Disabled' (Scored)	☐	☐
18.9.85.3	(L2) Ensure 'Prevent Internet Explorer security prompt for Windows Installer scripts' is set to 'Disabled' (Scored)	☐	☐
18.9.86	**Windows Logon Options**		
18.9.87	**Windows Mail**		
18.9.88	**Windows Media Center**		
18.9.89	**Windows Media Digital Rights Management**		
18.9.90	**Windows Media Player**		
18.9.91	**Windows Meeting Space**		
18.9.92	**Windows Messenger**		
18.9.93	**Windows Mobility Center**		
18.9.94	**Windows Movie Maker**		
18.9.95	**Windows PowerShell**		
18.9.95.1	(L1) Ensure 'Turn on PowerShell Script Block Logging' is set to 'Disabled' (Scored)	☐	☐
18.9.95.2	(L1) Ensure 'Turn on PowerShell Transcription' is set to 'Disabled' (Scored)	☐	☐
18.9.96	**Windows Reliability Analysis**		

Control		Set Correctly	
		Yes	No
18.9.97	**Windows Remote Management (WinRM)**		
18.9.97.1	**WinRM Client**		
18.9.97.1.1	(L1) Ensure 'Allow Basic authentication' is set to 'Disabled' (Scored)	☐	☐
18.9.97.1.2	(L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled' (Scored)	☐	☐
18.9.97.1.3	(L1) Ensure 'Disallow Digest authentication' is set to 'Enabled' (Scored)	☐	☐
18.9.97.2	**WinRM Service**		
18.9.97.2.1	(L1) Ensure 'Allow Basic authentication' is set to 'Disabled' (Scored)	☐	☐
18.9.97.2.2	(L2) Ensure 'Allow remote server management through WinRM' is set to 'Disabled' (Scored)	☐	☐
18.9.97.2.3	(L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled' (Scored)	☐	☐
18.9.97.2.4	(L1) Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled' (Scored)	☐	☐
18.9.98	**Windows Remote Shell**		
18.9.98.1	(L2) Ensure 'Allow Remote Shell Access' is set to 'Disabled' (Scored)	☐	☐
18.9.99	**Windows Security (formerly Windows Defender Security Center)**		
18.9.100	**Windows SideShow**		
18.9.101	**Windows System Resource Manager**		
18.9.102	**Windows Update**		
18.9.102.1	(L1) Ensure 'Configure Automatic Updates' is set to 'Enabled' (Scored)	☐	☐
18.9.102.2	(L1) Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day' (Scored)	☐	☐
18.9.102.3	(L1) Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled' (Scored)	☐	☐
19	**Administrative Templates (User)**		
19.1	**Control Panel**		
19.1.1	**Add or Remove Programs**		
19.1.2	**Display**		
19.1.3	**Personalization (formerly Desktop Themes)**		
19.1.3.1	(L1) Ensure 'Enable screen saver' is set to 'Enabled' (Scored)	☐	☐
19.1.3.2	(L1) Ensure 'Force specific screen saver: Screen saver executable name' is set to 'Enabled: scrnsave.scr' (Scored)	☐	☐

Control		Set Correctly	
		Yes	No
19.1.3.3	(L1) Ensure 'Password protect the screen saver' is set to 'Enabled' (Scored)	☐	☐
19.1.3.4	(L1) Ensure 'Screen saver timeout' is set to 'Enabled: 900 seconds or fewer, but not 0' (Scored)	☐	☐
19.2	**Desktop**		
19.3	**Network**		
19.4	**Shared Folders**		
19.5	**Start Menu and Taskbar**		
19.5.1	**Notifications**		
19.5.1.1	(L1) Ensure 'Turn off toast notifications on the lock screen' is set to 'Enabled' (Scored)	☐	☐
19.6	**System**		
19.6.1	**Ctrl+Alt+Del Options**		
19.6.2	**Display**		
19.6.3	**Driver Installation**		
19.6.4	**Folder Redirection**		
19.6.5	**Group Policy**		
19.6.6	**Internet Communication Management**		
19.6.6.1	**Internet Communication settings**		
19.6.6.1.1	(L2) Ensure 'Turn off Help Experience Improvement Program' is set to 'Enabled' (Scored)	☐	☐
19.7	**Windows Components**		
19.7.1	**Add features to Windows 8 / 8.1 / 10 (formerly Windows Anytime Upgrade)**		
19.7.2	**App runtime**		
19.7.3	**Application Compatibility**		
19.7.4	**Attachment Manager**		
19.7.4.1	(L1) Ensure 'Do not preserve zone information in file attachments' is set to 'Disabled' (Scored)	☐	☐
19.7.4.2	(L1) Ensure 'Notify antivirus programs when opening attachments' is set to 'Enabled' (Scored)	☐	☐
19.7.5	**AutoPlay Policies**		
19.7.6	**Backup**		
19.7.7	**Cloud Content**		
19.7.8	**Credential User Interface**		
19.7.9	**Data Collection and Preview Builds**		
19.7.10	**Desktop Gadgets**		
19.7.11	**Desktop Window Manager**		
19.7.12	**Digital Locker**		
19.7.13	**Edge UI**		

Control		Set Correctly	
		Yes	No
19.7.14	**File Explorer (formerly Windows Explorer)**		
19.7.15	**File Revocation**		
19.7.16	**IME**		
19.7.17	**Import Video**		
19.7.18	**Instant Search**		
19.7.19	**Internet Explorer**		
19.7.20	**Location and Sensors**		
19.7.21	**Microsoft Edge**		
19.7.22	**Microsoft Management Console**		
19.7.23	**Microsoft User Experience Virtualization**		
19.7.24	**NetMeeting**		
19.7.25	**Network Projector**		
19.7.26	**Network Sharing**		
19.7.26.1	(L1) Ensure 'Prevent users from sharing files within their profile.' is set to 'Enabled' (Scored)	☐	☐
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**		
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 Defender SmartScreen**		
19.7.39	**Windows Error Reporting**		
19.7.40	**Windows Hello for Business (formerly Microsoft Passport for Work)**		
19.7.41	**Windows Installer**		
19.7.41.1	(L1) Ensure 'Always install with elevated privileges' is set to 'Disabled' (Scored)	☐	☐
19.7.42	**Windows Logon Options**		
19.7.43	**Windows Mail**		
19.7.44	**Windows Media Center**		
19.7.45	**Windows Media Player**		
19.7.45.1	**Networking**		
19.7.45.2	**Playback**		

Control		Set Correctly	
		Yes	No
19.7.45.2.1	(L2) Ensure 'Prevent Codec Download' is set to 'Enabled' (Scored)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
01-31-2013	1.0.0	Initial Public Release
05-16-2016	2.0.0	Complete rewrite and reorganization of the benchmark.
01-31-2017	2.0.1	ADD – (L2) Ensure 'Allow remote server management through WinRM' is set to 'Disabled'. Ticket #581
01-31-2017	2.0.1	REMOVE – (L1) Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher from DC profile (retain only for MS profile). Ticket #583
01-31-2017	2.0.1	UPDATE of all "Default Value" entries to reflect default behavior instead of "Not Configured", and streamline of other recommendation text to simplify and increase readability. Ticket #584
01-31-2017	2.0.1	UPDATE for EMET v5.51 release (also caused removal of 19.7.12 EMET user-based section & renumbering of subsequent sections) Ticket #586
01-31-2017	2.0.1	REMOVE – (L1) Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled' from DC profile (retain only for MS profile). Ticket #590
01-31-2017	2.0.1	REMOVE – (L1) Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled' from DC profile (retain only for MS profile). Ticket #591

Date	Version	Changes for this version
01-31-2017	2.0.1	RENAME & RELOCATE "Microsoft Passport for Work" sections to "Windows Hello for Business" to reflect change in new Windows 10 R1607 & Server 2016 administrative templates. Ticket #595
01-31-2017	2.0.1	MERGE "SkyDrive" section into "OneDrive" section and rename to "OneDrive (formerly SkyDrive)" to reflect full consolidation in new Windows 10 R1607 & Server 2016 administrative templates. Ticket #596
01-31-2017	2.0.1	ADD all new sections from new Windows 10 R1607 & Server 2016 administrative templates. Causes some section renumbering. Ticket #597
01-31-2017	2.0.1	UPDATE – SkyDrive and OneDrive settings for better clarity between Next Generation Sync Client and legacy OneDrive client. Ticket #2846
01-31-2017	2.0.1	Added mappings to the CIS Critical Security Controls.
03-30-2018	2.1.0	UPDATE - 18.9.24 (L1) Ensure 'EMET 5.51' or higher is installed to EMET 5.52 Ticket #4725
03-30-2018	2.1.0	ADD - 18.9.69.8 (L2) Ensure 'Configure Watson events' is set to 'Disabled' Ticket #4726
03-30-2018	2.1.0	UPDATE - 17.5 (L1) Ensure 'Audit Account Lockout' is set to 'Success' to include 'Failure' Ticket #4729
03-30-2018	2.1.0	ADD - 17.7 (L1) Ensure 'Authorization Policy Change' is set to 'Success' Ticket #4731

Date	Version	Changes for this version
03-30-2018	2.1.0	UPDATE - 18.9.30 (L1) Ensure 'Configure Windows SmartScreen' is set to 'Enabled: Require approval from an administrator before running downloaded unknown software' to 'Enabled' Ticket #4732
03-30-2018	2.1.0	ADD - 18.4.4 (L1) Ensure 'Turn off multicast name resolution' is set to 'Enabled' (MS Only) Ticket #4840
03-30-2018	2.1.0	ADD - 18.4.4 (L1) Set 'NetBIOS node type' to 'P-node' (Ensure NetBT Parameter 'NodeType' is set to '0x2 (2)') (MS only) Ticket #4849
03-30-2018	2.1.0	UPDATE - 2.3.11.4 (L1) Ensure 'Network security: Configure encryption types allowed for Kerberos' is set to 'AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types' Ticket #5148
03-30-2018	2.1.0	UPDATE - 2.3.11.6 (L1) Ensure 'Network security: Force logoff when logon hours expire' is set to 'Enabled' to be Unscored Ticket #5353
03-30-2018	2.1.0	ADD - 18.3 (L1) Ensure 'Configure SMB v1 client' is set to 'Enabled: Bowser, MRxSmb20, NSI' Ticket #5358
03-30-2018	2.1.0	ADD - 18.3 (L1) Ensure 'Configure SMB v1 client driver' is set to 'Enabled: Disable driver' Ticket #5359
03-30-2018	2.1.0	ADD - 18.3 (L1) Ensure 'Configure SMB v1 server' is set to 'Disabled' Ticket #5361

Date	Version	Changes for this version
03-30-2018	2.1.0	ADD - 18.3 (L1) Ensure 'Enable Structured Exception Handling Overwrite Protection (SEHOP)' is set to 'Enabled' Ticket #5362
03-30-2018	2.1.0	UPDATE - 18.9.30.2 (L1) Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled: Warn' Ticket #5365
03-30-2018	2.1.0	UPDATE - Rename and Reorder '18.7 - SCM: Pass the Hash Mitigations' to '18.3 - MS Security Guide' Ticket #5416
03-30-2018	2.1.0	MOVE & RENAME - 18.9.30.2 (L1) Ensure 'Configure Windows SmartScreen' is set to 'Enabled' Ticket #5449
03-30-2018	2.1.0	REMOVE - 9.1.5 (L1) Ensure 'Windows Firewall: Domain: Settings: Apply local firewall rules' is set to 'Yes (default)' Ticket #5463
03-30-2018	2.1.0	REMOVE - 9.1.6 (L1) Ensure 'Windows Firewall: Domain: Settings: Apply local connection security rules' is set to 'Yes (default)' Ticket #5464
03-30-2018	2.1.0	REMOVE - 9.2.6 (L1) Ensure 'Windows Firewall: Private: Settings: Apply local connection security rules' is set to 'Yes (default)' Ticket #5465
03-30-2018	2.1.0	REMOVE - 9.2.5 (L1) Ensure 'Windows Firewall: Private: Settings: Apply local firewall rules' is set to 'Yes (default)' Ticket #5466

Date	Version	Changes for this version
03-30-2018	2.1.0	UPDATE - 9.3.4 (L1) Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'Yes' - change to 'No' Ticket #5467
03-30-2018	2.1.0	RENAME - 18.9.72 'Windows Defender' section to 'Windows Defender Antivirus' Ticket #5468
03-30-2018	2.1.0	ADD - New sections from Windows 10 Release 1703 Administrative Templates Ticket #5469
03-30-2018	2.1.0	REMOVE - 18.9.64.3 (L1) Ensure 'Turn off Automatic Download of updates on Win8 machines' is set to 'Disabled' Ticket #5567
03-30-2018	2.1.0	REMOVE - 18.9.64.4 (L1) Ensure 'Turn off the offer to update to the latest version of Windows' is set to 'Enabled' Ticket #5568
03-30-2018	2.1.0	REMOVE - 18.9.64.5 (L2) Ensure 'Turn off the Store application' is set to 'Enabled' Ticket #5569
03-30-2018	2.1.0	REMOVE - 18.8.21.1.1 (L2) Ensure 'Turn off access to the Store' is set to 'Enabled' Ticket #5570
03-30-2018	2.1.0	ADD - 17.6 (L1) Ensure 'Audit Other Object Access Events' is set to 'Success and Failure' Ticket #5643

Date	Version	Changes for this version
03-30-2018	2.1.0	UPDATE - 18.8.22.1 (L2 -> L1) Ensure 'Turn off downloading of print drivers over HTTP' is set to 'Enabled' Ticket #5644
03-30-2018	2.1.0	UPDATE - 18.8.22.1 (L2 -> L1) Ensure 'Turn off Internet download for Web publishing and online ordering wizards' is set to 'Enabled' Ticket #5645
03-30-2018	2.1.0	UPDATE - 18.8.22.1 (L2 -> L1) Ensure 'Turn off printing over HTTP' is set to 'Enabled' Ticket #5646
03-30-2018	2.1.0	UPDATE - 18.9.80.1 (L1) Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled: Warn' - change to 'Enabled: Warn and prevent bypass' Ticket #5649
03-30-2018	2.1.0	UPDATE - 2.2 (L1) Configure 'Deny access to this computer from the network' - remove 'Local account' from DC profile Ticket #5652
03-30-2018	2.1.0	UPDATE - 2.2 (L1) Ensure 'Deny log on through Remote Desktop Services' to include 'Guests, Local account' - remove 'Local account' from DC profile Ticket #5653
03-30-2018	2.1.0	REMOVE - 2.3.1 (L1) Ensure 'Accounts: Guest account status' is set to 'Disabled' from DC profile (ALL -> MS only) Ticket #5654
03-30-2018	2.1.0	REMOVE - 2.3.1 (L1) Ensure 'Accounts: Administrator account status' is set to 'Disabled' from DC profile (ALL -> MS only) Ticket #5655

Date	Version	Changes for this version
03-30-2018	2.1.0	REMOVE - 18.8.27 (L1) Ensure 'Enumerate local users on domain-joined computers' is set to 'Disabled' from DC profile (ALL -> MS only) Ticket #5656
03-30-2018	2.1.0	ADD - New sections from Windows 10 Release 1709 Administrative Templates Ticket #5658
03-30-2018	2.1.0	RENAME - 18.9.101.1 'Defer Windows Updates' section to 'Windows Update for Business' Ticket #5659
03-30-2018	2.1.0	RENAME - 18.5.11.1 'Windows Firewall' section to 'Windows Defender Firewall' Ticket #5660
03-30-2018	2.1.0	ADD - 18.9.76 (L1) Ensure 'Turn off Windows Defender AntiVirus' is set to 'Disabled' Ticket #5667
03-30-2018	2.1.0	ADD - 18.9.76.3 (L1) Ensure 'Configure local setting override for reporting to Microsoft MAPS' is set to 'Disabled' Ticket #5668
03-30-2018	2.1.0	ADD - 18.9.76.7 (L1) Ensure 'Turn on behavior monitoring' is set to 'Enabled' Ticket #5669
03-30-2018	2.1.0	ADD - 18.9.76.10 (L1) Ensure 'Scan removable drives' is set to 'Enabled' Ticket #5670
03-30-2018	2.1.0	ADD - 18.9.76.10 (L1) Ensure 'Turn on e-mail scanning' is set to 'Enabled' Ticket #5671

Date	Version	Changes for this version
03-30-2018	2.1.0	UPDATE & RENAME - 2.2 (L1) Configure 'Allow log on locally' to Ensure 'Allow log on locally' is set to 'Administrators' Ticket #5738
03-30-2018	2.1.0	MOVE - 18.9.39 (L2) Ensure 'Turn off Windows Location Provider' is set to 'Enabled' to 18.9.39.1 Ticket #5739
03-30-2018	2.1.0	ADD - 18.9.39 (L2) Ensure 'Turn off location' is set to 'Enabled' Ticket #5740
03-30-2018	2.1.0	ADD - 18.8.27 (L1) Ensure 'Turn off picture password sign-in' is set to 'Enabled' Ticket #5964
03-30-2018	2.1.0	ADD - 18.1.2.1 Missing sub-section "Handwriting personalization" Ticket #6049
03-30-2018	2.1.0	UPDATE - 18.8.33.6 (L2 -> L1) Ensure 'Require a password when a computer wakes (on battery)' is set to 'Enabled' Ticket #6077
03-30-2018	2.1.0	UPDATE - 18.8.33.6 (L2 -> L1) Ensure 'Require a password when a computer wakes (plugged in)' is set to 'Enabled' Ticket #6078
04-28-2020	2.2.0	ADD - 18.7.1 (L2) Ensure 'Turn off notifications network usage' is set to 'Enabled' Ticket #7587
04-28-2020	2.2.0	ADD - 18.8.4 (L1) Ensure 'Encryption Oracle Remediation' is set to 'Enabled: Force Updated Clients' Ticket #7588

Date	Version	Changes for this version
04-28-2020	2.2.0	ADD - 18.9.58.3.9 (L1) Ensure 'Require use of specific security layer for remote (RDP) connections' is set to 'Enabled: SSL' Ticket #7610
04-28-2020	2.2.0	ADD - 18.9.58.3.9 (L1) Ensure 'Require user authentication for remote connections by using Network Level Authentication' is set to 'Enabled' Ticket #7611
04-28-2020	2.2.0	UPDATE - 2.3.9 (L1) Ensure 'Microsoft network server: Amount of idle time required before suspending session' is set to '15 or fewer minute(s), but not 0' to allow 0 Ticket #7969
04-28-2020	2.2.0	UPDATE - 17.2 (L1) Ensure 'Audit Security Group Management' is set to 'Success and Failure' to include 'Success' Ticket #7971
04-28-2020	2.2.0	UPDATE - 17.5 (L1) Ensure 'Audit Account Lockout' is set to 'Success and Failure' to include 'Failure' Ticket #7972
04-28-2020	2.2.0	UPDATE - 17.7 (L1) Ensure 'Audit Audit Policy Change' is set to 'Success and Failure' to include 'Success' Ticket #7973
04-28-2020	2.2.0	UPDATE - 17.9 (L1) Ensure 'Audit Security System Extension' is set to 'Success and Failure' to include 'Success' Ticket #7974
04-28-2020	2.2.0	ADD - 17.6 (L1) Ensure 'Audit Detailed File Share' is set to include 'Failure' Ticket #7975

Date	Version	Changes for this version
04-28-2020	2.2.0	ADD - 17.7 (L1) Ensure 'Audit MPSSVC Rule-Level Policy Change' is set to 'Success and Failure' Ticket #7977
04-28-2020	2.2.0	ADD - 17.7 (L1) Ensure 'Audit Other Policy Change Events' is set to include 'Failure' Ticket #7978
04-28-2020	2.2.0	UPDATE - 18.8.22.1 (L1 -> L2) Ensure 'Turn off downloading of print drivers over HTTP' is set to 'Enabled' (should have been Turn off printing over HTTP) Ticket #7979
04-28-2020	2.2.0	REMOVE - 17.2 (L1) Ensure 'Audit Other Account Management Events' is set to 'Success and Failure' from MS profile (ALL -> DC Only) Ticket #8020
04-28-2020	2.2.0	UPDATE - 17.2 (L1) Ensure 'Audit Other Account Management Events' is set to 'Success and Failure' to include 'Success' (DC Only) Ticket #8021
04-28-2020	2.2.0	ADD - New sections from Windows 10 Release 1803 Administrative Templates Ticket #8053
04-28-2020	2.2.0	ADD - New sections from Windows 10 Release 1809 & Server 2019 Administrative Templates Ticket #8156
04-28-2020	2.2.0	UPDATE - 18.8.22.1 (L1 -> L2) Ensure 'Turn off printing over HTTP' is set to 'Enabled' Ticket #8861

Date	Version	Changes for this version
04-28-2020	2.2.0	REMOVE - 2.3.17 (L1) Ensure 'User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop' is set to 'Disabled' Ticket #8863
04-28-2020	2.2.0	ADD - 18.3 (L1) Ensure 'Extended Protection for LDAP Authentication (Domain Controllers only)' is set to 'Enabled: Enabled, always (recommended)' (DC Only) Ticket #8873
04-28-2020	2.2.0	ADD - 17.6 (L1) Ensure 'Audit File Share' is set to 'Success and Failure' Ticket #8878
04-28-2020	2.2.0	UPDATE - Split NGWS profile into separate MS- and DC-specific profiles Ticket #8881
04-28-2020	2.2.0	UPDATE - 18.8.22.1 (L2 -> L1) Ensure 'Turn off downloading of print drivers over HTTP' is set to 'Enabled' Ticket #8897
04-28-2020	2.2.0	UPDATE - 17.2 (L1) Ensure 'Audit Distribution Group Management' is set to 'Success and Failure' TO include 'Success' (DC Only) Ticket #9112
04-28-2020	2.2.0	UPDATE - 17.4 (L1) Ensure 'Audit Directory Service Access' is set to 'Success and Failure' TO include 'Failure' (DC Only) Ticket #9113
04-28-2020	2.2.0	UPDATE - 17.4 (L1) Ensure 'Audit Directory Service Changes' is set to 'Success and Failure' TO include 'Success' (DC Only) Ticket #9114

Date	Version	Changes for this version
04-28-2020	2.2.0	REMOVE - 17.2 (L1) Ensure 'Audit Computer Account Management' is set to 'Success and Failure' from MS profile (ALL -> DC Only) Ticket #9115
04-28-2020	2.2.0	UPDATE - 17.2 (L1) Ensure 'Audit Computer Account Management' is set to 'Success and Failure' TO include 'Success' (DC Only) Ticket #9116
04-28-2020	2.2.0	ADD - New sections from Windows 10 Release 1903 Administrative Templates Ticket #9564
04-28-2020	2.2.0	MOVE & RENAME - 18.5.4 (L1) Set 'NetBIOS node type' TO 18.3 (L1) Ensure 'NetBT NodeType configuration' is set to 'Enabled: P-node (recommended)' Ticket #9566
04-28-2020	2.2.0	UPDATE - 18.3 (L1) Ensure 'NetBT NodeType configuration' is set to 'Enabled: P-node (recommended)' (Add to DC profile) Ticket #9567
04-28-2020	2.2.0	UPDATE - 18.5.4 (L1) Ensure 'Turn off multicast name resolution' is set to 'Enabled' (Add to DC profile) Ticket # 9568
04-28-2020	2.2.0	ADD - 17.1 (L1) Ensure 'Audit Kerberos Authentication Service' is set to 'Success and Failure' (DC Only) Ticket #9569
04-28-2020	2.2.0	ADD - 17.1 (L1) Ensure 'Audit Kerberos Service Ticket Operations' is set to 'Success and Failure' (DC Only) Ticket #9570