Security Benchmarks™
A DIVISION OF CENTER FOR INTERNET SECURITY

CIS Microsoft Windows Server 2003

v3.0.0 - 10-04-2013

The CIS Security Benchmarks division provides consensus-oriented information security products, services, tools, metrics, suggestions, and recommendations (the "SB Products") as a public service to Internet users worldwide. Downloading or using SB Products in any way signifies and confirms your acceptance of and your binding agreement to these CIS Security Benchmarks Terms of Use.

CIS SECURITY BENCHMARKS TERMS OF USE

BOTH CIS SECURITY BENCHMARKS DIVISION MEMBERS AND NON-MEMBERS MAY:

- Download, install, and use each of the SB Products on a single computer, and/or
- Print one or more copies of any SB Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, but only if each such copy is printed in its entirety and is kept intact, including without limitation the text of these CIS Security Benchmarks Terms of Use.

UNDER THE FOLLOWING TERMS AND CONDITIONS:

- **SB Products Provided As Is**. CIS is providing the SB Products "as is" and "as available" without: (1) any representations, warranties, or covenants of any kind whatsoever (including the absence of any warranty regarding: (a) the effect or lack of effect of any SB Product on the operation or the security of any network, system, software, hardware, or any component of any of them, and (b) the accuracy, utility, reliability, timeliness, or completeness of any SB Product); or (2) the responsibility to make or notify you of any corrections, updates, upgrades, or fixes.
- **Intellectual Property and Rights Reserved**. You are not acquiring any title or ownership rights in or to any SB Product, and full title and all ownership rights to the SB Products remain the exclusive property of CIS. All rights to the SB Products not expressly granted in these Terms of Use are hereby reserved.
- **Restrictions**. You acknowledge and agree that you may not: (1) decompile, dis-assemble, alter, reverse engineer, or otherwise attempt to derive the source code for any software SB Product that is not already in the form of source code; (2) distribute, redistribute, sell, rent, lease, sublicense or otherwise transfer or exploit any rights to any SB Product in any way or for any purpose; (3) post any SB Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device; (4) remove from or alter these CIS Security Benchmarks Terms of Use on any SB Product; (5) remove or alter any proprietary notices on any SB Product; (6) use any SB Product or any component of an SB Product with any derivative works based directly on an SB Product or any component of an SB Product; (7) use any SB Product or any component of an SB Product with other products or applications that are directly and specifically dependent on such SB Product or any component for any part of their functionality; (8) represent or claim a particular level of compliance or consistency with any SB Product; or (9) facilitate or otherwise aid other individuals or entities in violating these CIS Security Benchmarks Terms of Use.
- **Your Responsibility to Evaluate Risks**. You acknowledge and agree that: (1) no network, system, device, hardware, software, or component can be made fully secure; (2) you have the sole responsibility to evaluate the risks and benefits of the SB Products to your particular circumstances and requirements; and (3) CIS is not assuming any of the liabilities associated with your use of any or all of the SB Products.
- **CIS Liability**. You acknowledge and agree that neither CIS nor any of its employees, officers, directors, agents or other service providers has or will have any liability to you whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages that arise out of or are connected in any way with your use of any SB Product.
- **Indemnification**. You agree to indemnify, defend, and hold CIS and all of CIS's employees, officers, directors, agents and other service providers harmless from and against any liabilities, costs and expenses incurred by any of them in connection with your violation of these CIS Security Benchmarks Terms of Use.
- **Jurisdiction**. You acknowledge and agree that: (1) these CIS Security Benchmarks Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland; (2) any action at law or in equity arising out of or relating to these CIS Security Benchmarks Terms of Use shall be filed only in the courts located in the State of Maryland; and (3) you hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action.
- **U.S. Export Control and Sanctions laws**. Regarding your use of the SB Products with any non-U.S. entity or country, you acknowledge that it is your responsibility to understand and abide by all U.S. sanctions and export control laws as set from time to time by the U.S. Bureau of Industry and Security (BIS) and the U.S. Office of Foreign Assets Control (OFAC).

SPECIAL RULES FOR CIS MEMBER ORGANIZATIONS: CIS reserves the right to create special rules for: (1) CIS Members; and (2) Non-Member organizations and individuals with which CIS has a written contractual relationship. CIS hereby grants to each CIS Member Organization in good standing the right to distribute the SB Products within such Member's own organization, whether by manual or electronic means. Each such Member Organization acknowledges and agrees that the foregoing grants in this paragraph are subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Table of Contents

Overview 16

Recommendations 20

1 Computer Configuration 20

1.1 Windows Settings 20

1.1.1 Security Settings 20

1.1.1.1 Account Policies 20

1.1.1.1.1 Kerberos Policy 20

1.1.1.1.1.1 Configure 'Maximum lifetime for service ticket' (Not Scored) 20

1.1.1.1.1.2 Configure 'Enforce user logon restrictions' (Not Scored) 21

1.1.1.1.1.3 Configure 'Maximum lifetime for user ticket' (Not Scored) 22

1.1.1.1.1.4 Configure 'Maximum tolerance for computer clock synchronization' (Not Scored) 23

1.1.1.1.1.5 Configure 'Maximum lifetime for user ticket renewal' (Not Scored) 24

1.1.1.2 Local Policies 25

1.1.1.2.1 Security Options 25

1.1.1.2.1.1 Set 'Domain controller: Allow server operators to schedule tasks' to 'Disabled' (Scored) 25

1.1.1.2.1.2 Configure 'Domain controller: Allow server operators to schedule tasks' (Not Scored) 26

1.1.1.2.1.3 Set 'Accounts: Guest account status' to 'Disabled' (Scored) 28

1.1.1.2.1.4 Set 'Accounts: Limit local account use of blank passwords to console logon only' to 'Enabled' (Scored) 29

1.1.1.2.1.5 Set 'Domain controller: Refuse machine account password changes' to 'Disabled' (Scored) 30

1.1.1.2.1.6 Configure 'Domain controller: Refuse machine account password changes' (Not Scored) 31

1.1.1.2.1.7 Set 'Accounts: Administrator account status' to 'Disabled' (Scored) 32

1.1.1.2.1.8 Set 'System objects: Default owner for objects created by members of the Administrators group' to 'Object creator' (Scored) 33

1.1.1.2.1.9 Set 'Network access: Shares that can be accessed anonymously' to '' (Scored) 34
1.1.1.2.1.10 Set 'Network access: Shares that can be accessed anonymously' to 'None' (Scored) 35
1.1.1.2.1.11 Set 'Interactive logon: Smart card removal behavior' to 'Lock Workstation' (Scored) 36
1.1.1.2.1.12 Set 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' to 'Require message integrity,Require message confidentiality,Require NTLMv2 session security,Require 128-bit encryption' (Scored) 37
1.1.1.2.1.13 Set 'Devices: Prevent users from installing printer drivers' to 'Enabled' (Scored) 39
1.1.1.2.1.14 Set 'Devices: Unsigned driver installation behavior' to 'Warn but allow installation' (Scored) 40
1.1.1.2.1.15 Set 'Recovery console: Allow floppy copy and access to all drives and all folders' to 'Disabled' (Scored) 41
1.1.1.2.1.16 Set 'MSS: (DisableSavePassword) Prevent the dial-up password from being saved (recommended)' to 'Enabled' (Scored) 42
1.1.1.2.1.17 Set 'Network access: Restrict anonymous access to Named Pipes and Shares' to 'Enabled' (Scored) 43
1.1.1.2.1.18 Set 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' to '90' (Scored) 44
1.1.1.2.1.19 Set 'MSS: (SynAttackProtect) Syn attack protection level (protects against DoS)' to 'Connections time out sooner if a SYN attack is detected' (Scored) 45
1.1.1.2.1.20 Set 'System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies' to 'Enabled' (Scored) 46
1.1.1.2.1.21 Set 'MSS: (AutoShareServer) Enable Administrative Shares (recommended except for highly secure environments)' to 'Enabled' (Scored) 47
1.1.1.2.1.22 Set 'Shutdown: Clear virtual memory pagefile' to 'Disabled' (Scored) 48
1.1.1.2.1.23 Set 'Domain member: Disable machine account password changes' to 'Disabled' (Scored) 49
1.1.1.2.1.24 Set 'Microsoft network server: Amount of idle time required before suspending session' to '15' (Scored) 50
1.1.1.2.1.25 Set 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' to 'Enabled' (Scored) 51

1.1.1.2.1.26 Configure 'Devices: Restrict CD-ROM access to locally logged-on user only' (Not Scored) 53

1.1.1.2.1.27 Set 'MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds' to '300000 or 5 minutes (recommended)' (Scored) 54

1.1.1.2.1.28 Set 'Shutdown: Allow system to be shut down without having to log on' to 'Disabled' (Scored) 55

1.1.1.2.1.29 Set 'Interactive logon: Do not display last user name' to 'Enabled' (Scored) 56

1.1.1.2.1.30 Set 'Network security: LAN Manager authentication level' to 'Send NTLMv2 response only. Refuse LM & NTLM' (Scored) 57

1.1.1.2.1.31 Configure 'DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax' (Not Scored) 59

1.1.1.2.1.32 Configure 'MSS: (Hidden) Hide Computer From the Browse List (not recommended except for highly secure environments)' (Not Scored) 61

1.1.1.2.1.33 Set 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' to 'Disabled' (Scored) 63

1.1.1.2.1.34 Set 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' to 'Require message integrity,Require message confidentiality,Require NTLMv2 session security,Require 128-bit encryption' (Scored) 64

1.1.1.2.1.35 Set 'System objects: Require case insensitivity for non-Windows subsystems' to 'Enabled' (Scored) 65

1.1.1.2.1.36 Configure 'DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax' (Not Scored) 66

1.1.1.2.1.37 Set 'System settings: Optional subsystems' to '' (Scored) 68

1.1.1.2.1.38 Set 'Devices: Allowed to format and eject removable media' to 'Administrators' (Scored) 69

1.1.1.2.1.39 Set 'Microsoft network client: Digitally sign communications (always)' to 'Enabled' (Scored) 70

1.1.1.2.1.40 Set 'Interactive logon: Prompt user to change password before expiration' to '14' (Scored) 72

1.1.1.2.1.41 Set 'Domain member: Maximum machine account password age' to '30' (Scored) 73

1.1.1.2.1.42 Set 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' to 'Enabled' (Scored) 74

1.1.1.2.1.43 Configure 'Interactive logon: Display user information when the session is locked' (Not Scored) 75
1.1.1.2.1.44 Set 'MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)' to '3' (Scored) 76
1.1.1.2.1.45 Set 'Domain member: Digitally sign secure channel data (when possible)' to 'Enabled' (Scored) 77
1.1.1.2.1.46 Set 'Domain member: Digitally encrypt secure channel data (when possible)' to 'Enabled' (Scored) 78
1.1.1.2.1.47 Configure 'Domain controller: LDAP server signing requirements' (Not Scored) 80
1.1.1.2.1.48 Set 'Microsoft network client: Send unencrypted password to third-party SMB servers' to 'Disabled' (Scored) 81
1.1.1.2.1.49 Set 'Interactive logon: Do not require CTRL+ALT+DEL' to 'Disabled' (Scored) 82
1.1.1.2.1.50 Configure 'Interactive logon: Message title for users attempting to log on' (Not Scored) 83
1.1.1.2.1.51 Configure 'Interactive logon: Message text for users attempting to log on' (Not Scored) 84
1.1.1.2.1.52 Set 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)' to '0' (Scored) 86
1.1.1.2.1.53 Set 'Microsoft network client: Digitally sign communications (if server agrees)' to 'Enabled' (Scored) 87
1.1.1.2.1.54 Set 'Domain member: Digitally encrypt or sign secure channel data (always)' to 'Enabled' (Scored) 88
1.1.1.2.1.55 Set 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)' to 'Enabled' (Scored) 90
1.1.1.2.1.56 Set 'Network security: Do not store LAN Manager hash value on next password change' to 'Enabled' (Scored) 91
1.1.1.2.1.57 Set 'Network access: Remotely accessible registry paths and sub-paths' to 'System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Services\Eventlog Software\Microsoft\OLAP Server Software\Microsoft\Windows NT\CurrentVersion\Print Sof (Scored) 92
1.1.1.2.1.58 Configure 'System cryptography: Force strong key protection for user keys stored on the computer' (Not Scored) 93

1.1.1.2.1.59 Set 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' to 'Highest protection, source routing is completely disabled' (Scored) 95

1.1.1.2.1.60 Set 'MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)' to 'Disabled' (Scored) 96

1.1.1.2.1.61 Set 'MSS: (TcpMaxConnectResponseRetransmissions) SYN-ACK retransmissions when a connection request is not acknowledged' to '3 & 6 seconds, half-open connections dropped after 21 seconds' (Scored) 97

1.1.1.2.1.62 Set 'Microsoft network server: Disconnect clients when logon hours expire' to 'Enabled' (Scored) 98

1.1.1.2.1.63 Set 'Network access: Let Everyone permissions apply to anonymous users' to 'Disabled' (Scored) 99

1.1.1.2.1.64 Set 'Microsoft network server: Digitally sign communications (always)' to 'Enabled' (Scored) 100

1.1.1.2.1.65 Set 'Network security: LDAP client signing requirements' to 'Negotiate signing' (Scored) 101

1.1.1.2.1.66 Set 'Devices: Allow undock without having to log on' to 'Disabled' (Scored) 103

1.1.1.2.1.67 Set 'Audit: Audit the access of global system objects' to 'Disabled' (Scored) 104

1.1.1.2.1.68 Set 'MSS: (AutoReboot) Allow Windows to automatically restart after a system crash (recommended except for highly secure environments)' to 'Enabled' (Scored) 105

1.1.1.2.1.69 Set 'Interactive logon: Require smart card' to 'Disabled' (Scored) 106

1.1.1.2.1.70 Configure 'Devices: Restrict floppy access to locally logged-on user only' (Not Scored) 107

1.1.1.2.1.71 Set 'Network access: Allow anonymous SID/Name translation' to 'Disabled' (Scored) 108

1.1.1.2.1.72 Set 'Domain member: Require strong (Windows 2000 or later) session key' to 'Enabled' (Scored) 109

1.1.1.2.1.73 Set 'Network access: Remotely accessible registry paths' to 'System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications Software\Microsoft\Windows NT\CurrentVersion' (Scored) 110

1.1.1.2.1.74 Set 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' to '0' (Scored) 112
1.1.1.2.1.75 Configure 'Network access: Named Pipes that can be accessed anonymously' (Not Scored) 113
1.1.1.2.1.76 Set 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' to 'Enabled' (Scored) 114
1.1.1.2.1.77 Set 'Recovery console: Allow automatic administrative logon' to 'Disabled' (Scored) 115
1.1.1.2.1.78 Set 'Audit: Shut down system immediately if unable to log security audits' to 'Disabled' (Scored) 116
1.1.1.2.1.79 Set 'Microsoft network server: Digitally sign communications (if client agrees)' to 'Enabled' (Scored) 117
1.1.1.2.1.80 Set 'Network access: Sharing and security model for local accounts' to 'Classic - local users authenticate as themselves' (Scored) 119
1.1.1.2.1.81 Set 'Network access: Do not allow anonymous enumeration of SAM accounts' to 'Enabled' (Scored) 120
1.1.1.2.1.82 Set 'Interactive logon: Require Domain Controller authentication to unlock workstation' to 'Enabled' (Scored) 121
1.1.1.2.1.83 Set 'Network access: Do not allow storage of credentials or .NET Passports for network authentication' to 'Enabled' (Scored) 122
1.1.1.2.1.84 Set 'MSS: (EnableDeadGWDetect) Allow automatic detection of dead network gateways (could lead to DoS)' to 'Disabled' (Scored) 123
1.1.1.2.1.85 Set 'System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing' to 'Disabled' (Scored) 124
1.1.1.2.1.86 Set 'Audit: Audit the use of Backup and Restore privilege' to 'Disabled' (Scored) 126
1.1.1.2.1.87 Set 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' to 'Disabled' (Scored) 127
1.1.1.2.1.88 Set 'MSS: (NoDefaultExempt) Configure IPSec exemptions for various types of network traffic.' to 'Only ISAKMP is exempt (recommended for Windows Server 2003)' (Scored) 128
1.1.1.2.2 Audit Policy 129
1.1.1.2.2.1 Set 'Audit directory service access' to 'Failure' (Scored) 130
1.1.1.2.2.2 Configure 'Audit directory service access' (Not Scored) 131

1.1.1.2.2.3 Set 'Audit account logon events' to 'Success, Failure' (Scored) 132
1.1.1.2.2.4 Set 'Audit logon events' to 'Success, Failure' (Scored) 134
1.1.1.2.2.5 Set 'Audit process tracking' to 'No Auditing' (Scored) 135
1.1.1.2.2.6 Set 'Audit account management' to 'Success, Failure' (Scored) 136
1.1.1.2.2.7 Set 'Audit policy change' to 'Success' (Scored) 138
1.1.1.2.2.8 Set 'Audit system events' to 'Success' (Scored) 140
1.1.1.2.2.9 Set 'Audit privilege use' to 'Failure' (Scored) 141
1.1.1.2.2.10 Configure 'Audit object access' (Not Scored) 142
1.1.1.2.3 User Rights Assignment 143
1.1.1.2.3.1 Set 'Allow log on through Terminal Services' to 'Administrators' (Scored) 143
1.1.1.2.3.2 Set 'Allow log on through Terminal Services' to 'Administrators, Remote desktop Users' (Scored) 145
1.1.1.2.3.3 Set 'Take ownership of files or other objects' to 'Administrators' (Scored) 146
1.1.1.2.3.4 Set 'Enable computer and user accounts to be trusted for delegation' to 'Administrators' (Scored) 147
1.1.1.2.3.5 Configure 'Enable computer and user accounts to be trusted for delegation' (Not Scored) 147
1.1.1.2.3.6 Set 'Remove computer from docking station' to 'Administrators' (Scored) 148
1.1.1.2.3.7 Configure 'Create permanent shared objects' (Not Scored) 149
1.1.1.2.3.8 Set 'Debug programs' to 'Administrators' (Scored) 150
1.1.1.2.3.9 Configure 'Load and unload device drivers' (Not Scored) 152
1.1.1.2.3.10 Set 'Adjust memory quotas for a process' to 'Administrators, LOCAL SERVICE, NETWORK SERVICE' (Scored) 153
1.1.1.2.3.11 Configure 'Generate security audits' (Not Scored) 154
1.1.1.2.3.12 Set 'Shut down the system' to 'Administrators' (Scored) 155
1.1.1.2.3.13 Configure 'Increase scheduling priority' (Not Scored) 156
1.1.1.2.3.14 Set 'Replace a process level token' to 'LOCAL SERVICE, NETWORK SERVICE' (Scored) 157
1.1.1.2.3.15 Configure 'Add workstations to domain' (Not Scored) 158

1.1.1.2.3.16 Configure 'Change the system time' (Not Scored) 159
1.1.1.2.3.17 Configure 'Restore files and directories' (Not Scored) 160
1.1.1.2.3.18 Configure 'Create a token object' (Not Scored) 162
1.1.1.2.3.19 Configure 'Synchronize directory service data' (Not Scored) 163
1.1.1.2.3.20 Set 'Profile system performance' to 'Administrators' (Scored) 163
1.1.1.2.3.21 Configure 'Access this computer from the network' (Not Scored) 164
1.1.1.2.3.22 Set 'Profile single process' to 'Administrators' (Scored) 166
1.1.1.2.3.23 Configure 'Impersonate a client after authentication' (Not Scored) 167
1.1.1.2.3.24 Set 'Create a pagefile' to 'Administrators' (Scored) 168
1.1.1.2.3.25 Set 'Deny log on as a batch job' to 'Guests' (Scored) 169
1.1.1.2.3.26 Set 'Deny log on through Terminal Services' to 'Guests' (Scored) 170
1.1.1.2.3.27 Configure 'Act as part of the operating system' (Not Scored) 171
1.1.1.2.3.28 Configure 'Back up files and directories' (Not Scored) 172
1.1.1.2.3.29 Set 'Log on as a service' to 'NETWORK SERVICE' (Scored) 173
1.1.1.2.3.30 Set 'Deny access to this computer from the network' to 'ANONYMOUS LOGON, Guests' (Scored) 174
1.1.1.2.3.31 Configure 'Perform volume maintenance tasks' (Not Scored) 175
1.1.1.2.3.32 Configure 'Deny log on locally' (Not Scored) 175
1.1.1.2.3.33 Set 'Allow log on locally' to 'Administrators' (Scored) 176
1.1.1.2.3.34 Configure 'Create global objects' (Not Scored) 177
1.1.1.2.3.35 Configure 'Bypass traverse checking' (Not Scored) 178
1.1.1.2.3.36 Configure 'Deny log on as a service' (Not Scored) 179
1.1.1.2.3.37 Set 'Manage auditing and security log' to 'Administrators' (Scored) 180
1.1.1.2.3.38 Configure 'Lock pages in memory' (Not Scored) 181
1.1.1.2.3.39 Configure 'Force shutdown from a remote system' (Not Scored) 182
1.1.1.2.3.40 Set 'Modify firmware environment values' to 'Administrators' (Scored) 183
1.1.1.2.3.41 Configure 'Log on as a batch job' (Not Scored) 184
1.1.1.3 Event Log 185
1.1.1.3.1 Set 'Retention method for system log' to 'Overwrites events as needed' (Scored) 185
1.1.1.3.2 Set 'Maximum application log size' to '16384' (Scored) 186

1.1.1.3.3 Set 'Retention method for security log' to 'Overwrites events as needed' (Scored) 187
1.1.1.3.4 Set 'Maximum system log size' to '16384' (Scored) 188
1.1.1.3.5 Set 'Maximum security log size' to '81920' (Scored) 189
1.1.1.3.6 Set 'Retention method for application log' to 'Overwrites events as needed' (Scored) 191
1.1.1.3.7 Configure 'Retain system log' (Not Scored) 192
1.1.1.3.8 Configure 'Retain security log' (Not Scored) 192
1.1.1.3.9 Configure 'Retain application log' (Not Scored) 193
1.2 Administrative Templates 194
1.2.1 Network 194
1.2.1.1 Network Connections 194
1.2.1.1.1 Windows Firewall 194
1.2.1.1.1.1 Standard Profile 194
1.2.1.1.1.1.1 Configure 'Windows Firewall: Allow ICMP exceptions' (Not Scored) 194
1.2.1.1.1.1.2 Configure 'Windows Firewall: Define inbound port exceptions' (Not Scored) 196
1.2.1.1.1.1.3 Configure 'Windows Firewall: Prohibit unicast response to multicast or broadcast requests' (Not Scored) 197
1.2.1.1.1.1.4 Configure 'Windows Firewall: Allow local program exceptions' (Not Scored) 198
1.2.1.1.1.1.5 Configure 'Windows Firewall: Allow inbound remote administration exception' (Not Scored) 199
1.2.1.1.1.1.6 Configure 'Windows Firewall: Allow inbound Remote Desktop exceptions' (Not Scored) 200
1.2.1.1.1.1.7 Configure 'WF_IcmpSettings_AllowOutboundSourceQuench' (Not Scored) 201
1.2.1.1.1.1.8 Configure 'WF_IcmpSettings_AllowOutboundParameterProblem' (Not Scored) 202
1.2.1.1.1.1.9 Configure 'Windows Firewall: Allow inbound UPnP framework exceptions' (Not Scored) 203
1.2.1.1.1.1.10 Configure 'WF_IcmpSettings_AllowInboundMaskRequest' (Not Scored) 204

1.2.1.1.1.1.11 Configure 'WF_IcmpSettings_AllowRedirect' (Not Scored) 205
1.2.1.1.1.1.12 Configure 'WF_IcmpSettings_AllowOutboundDestinationUnreachable' (Not Scored) 205
1.2.1.1.1.1.13 Configure 'WF_IcmpSettings_AllowOutboundTimeExceeded' (Not Scored) 206
1.2.1.1.1.1.14 Configure 'Windows Firewall: Allow inbound file and printer sharing exception' (Not Scored) 207
1.2.1.1.1.1.15 Configure 'Windows Firewall: Define inbound program exceptions' (Not Scored) 208
1.2.1.1.1.1.16 Configure 'WF_IcmpSettings_AllowInboundRouterRequest' (Not Scored) 209
1.2.1.1.1.1.17 Configure 'Windows Firewall: Allow local port exceptions' (Not Scored) 210
1.2.1.1.1.1.18 Configure 'WF_IcmpSettings_AllowInboundEchoRequest' (Not Scored) 211
1.2.1.1.1.1.19 Configure 'WF_IcmpSettings_AllowOutboundPacketTooBig' (Not Scored) 212
1.2.1.1.1.1.20 Configure 'Windows Firewall: Prohibit notifications' (Not Scored) 213
1.2.1.1.1.1.21 Configure 'WF_IcmpSettings_AllowInboundTimestampRequest' (Not Scored) 214
1.2.1.1.1.1.22 Configure 'Windows Firewall: Do not allow exceptions' (Not Scored) 215
1.2.1.1.1.1.23 Configure 'Windows Firewall: Protect all network connections' (Not Scored) 216
1.2.1.1.1.2 Domain Profile 217
1.2.1.1.1.2.1 Configure 'Windows Firewall: Allow inbound UPnP framework exceptions' (Not Scored) 217
1.2.1.1.1.2.2 Configure 'Windows Firewall: Do not allow exceptions' (Not Scored) 218
1.2.1.1.1.2.3 Configure 'Windows Firewall: Allow local program exceptions' (Not Scored) 219
1.2.1.1.1.2.4 Configure 'WF_IcmpSettings_AllowOutboundPacketTooBig' (Not Scored) 220
1.2.1.1.1.2.5 Configure 'Windows Firewall: Allow local port exceptions' (Not Scored) 221

1.2.1.1.1.2.6 Configure 'Windows Firewall: Allow inbound remote administration exception' (Not Scored) 222
1.2.1.1.1.2.7 Configure 'Windows Firewall: Allow inbound file and printer sharing exception' (Not Scored) 224
1.2.1.1.1.2.8 Configure 'WF_IcmpSettings_AllowOutboundSourceQuench' (Not Scored) 225
1.2.1.1.1.2.9 Configure 'WF_IcmpSettings_AllowOutboundTimeExceeded' (Not Scored) 226
1.2.1.1.1.2.10 Configure 'Windows Firewall: Allow ICMP exceptions' (Not Scored) 227
1.2.1.1.1.2.11 Configure 'WF_IcmpSettings_AllowOutboundParameterProblem' (Not Scored) 228
1.2.1.1.1.2.12 Configure 'WF_IcmpSettings_AllowInboundEchoRequest' (Not Scored) 229
1.2.1.1.1.2.13 Configure 'WF_IcmpSettings_AllowInboundMaskRequest' (Not Scored) 230
1.2.1.1.1.2.14 Configure 'WF_IcmpSettings_AllowRedirect' (Not Scored) 231
1.2.1.1.1.2.15 Configure 'Windows Firewall: Prohibit notifications' (Not Scored) 232
1.2.1.1.1.2.16 Configure 'Windows Firewall: Define inbound port exceptions' (Not Scored) 233
1.2.1.1.1.2.17 Configure 'WF_IcmpSettings_AllowInboundRouterRequest' (Not Scored) 234
1.2.1.1.1.2.18 Configure 'WF_IcmpSettings_AllowOutboundDestinationUnreachable' (Not Scored) 235
1.2.1.1.1.2.19 Configure 'Windows Firewall: Protect all network connections' (Not Scored) 236
1.2.1.1.1.2.20 Configure 'Windows Firewall: Prohibit unicast response to multicast or broadcast requests' (Not Scored) 237
1.2.1.1.1.2.21 Configure 'Windows Firewall: Define inbound program exceptions' (Not Scored) 238
1.2.1.1.1.2.22 Configure 'WF_IcmpSettings_AllowInboundTimestampRequest' (Not Scored) 239
1.2.1.1.1.2.23 Configure 'Windows Firewall: Allow inbound Remote Desktop exceptions' (Not Scored) 240
1.2.2 System 241

1.2.2.1 Remote Assistance 241
1.2.2.1.1 Configure 'RA_Solicit_ExpireUnits_List' (Not Scored) 241
1.2.2.1.2 Configure 'RA_Solicit_Control_List' (Not Scored) 241
1.2.2.1.3 Configure 'Offer Remote Assistance' (Not Scored) 242
1.2.2.1.4 Configure 'RA_Solicit_ExpireValue_Edt' (Not Scored) 243
1.2.2.1.5 Configure 'RA_Solicit_Mailto_List' (Not Scored) 244
1.2.2.1.6 Configure 'Solicited Remote Assistance' (Not Scored) 245
1.2.2.2 Internet Communication Management 247
1.2.2.2.1 Internet Communication settings 247
1.2.2.2.1.1 Configure 'Turn off Windows Update device driver searching' (Not Scored) 247
1.2.2.2.1.2 Configure 'Turn off Search Companion content file updates' (Not Scored) 248
1.2.2.2.1.3 Configure 'Turn off Internet download for Web publishing and online ordering wizards' (Not Scored) 249
1.2.2.2.1.4 Configure 'Turn off the Windows Messenger Customer Experience Improvement Program' (Not Scored) 250
1.2.2.2.1.5 Configure 'Turn off printing over HTTP' (Not Scored) 251
1.2.2.2.1.6 Configure 'Turn off the “Publish to Web” task for files and folders' (Not Scored) 251
1.2.2.2.1.7 Configure 'Turn off downloading of print drivers over HTTP' (Not Scored) 252
1.2.2.3 Group Policy 253
1.2.2.3.1 Configure 'Registry policy processing' (Not Scored) 253
1.2.2.3.2 Configure 'CSE_NOBACKGROUND10' (Not Scored) 254
1.2.2.3.3 Configure 'CSE_NOCHANGES10' (Not Scored) 255
1.2.2.4 Remote Procedure Call 256
1.2.2.4.1 Configure 'RPC Endpoint Mapper Client Authentication' (Not Scored) 256
1.2.2.4.2 Configure 'Restrictions for Unauthenticated RPC clients' (Not Scored) 257
1.2.2.5 Logon 258
1.2.2.5.1 Configure 'Do not process the legacy run list' (Not Scored) 258
1.2.2.5.2 Configure 'Do not process the run once list' (Not Scored) 259
1.2.3 Windows Components 260

1.2.3.1 AutoPlay Policies 260
1.2.3.1.1 Set 'Turn off Autoplay' to 'Enabled:All drives' (Scored) 261
1.2.3.2 Windows Update 261
1.2.3.2.1 Configure 'AutoUpdateSchDay' (Not Scored) 262
1.2.3.2.2 Configure 'Specify intranet Microsoft update service location' (Not Scored) 262
1.2.3.2.3 Configure 'No auto-restart with logged on users for scheduled automatic updates installations' (Not Scored) 264
1.2.3.2.4 Configure 'CorpWUURL' (Not Scored) 265
1.2.3.2.5 Configure 'Configure Automatic Updates' (Not Scored) 266
1.2.3.2.6 Configure 'Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box' (Not Scored) 267
1.2.3.2.7 Configure 'AutoUpdateSchTime' (Not Scored) 268
1.2.3.2.8 Configure 'Do not adjust default option to 'Install Updates and Shut Down' in Shut Down Windows dialog box' (Not Scored) 268
1.2.3.2.9 Configure 'Reschedule Automatic Updates scheduled installations' (Not Scored) 269
1.2.3.2.10 Configure 'CorpWUStatusURL' (Not Scored) 271
1.2.3.2.11 Configure 'AutoUpdateMode' (Not Scored) 271
1.2.3.3 Windows Messenger 272
1.2.3.3.1 Configure 'Do not allow Windows Messenger to be run' (Not Scored) 272
1.2.3.4 Remote Desktop Services 273
1.2.3.4.1 Remote Desktop Connection Client 273
1.2.3.4.1.1 Configure 'Do not allow passwords to be saved' (Not Scored) 273
1.2.3.4.2 Remote Desktop Session Host 274
1.2.3.4.2.1 Device and Resource Redirection 274
1.2.3.4.2.1.1 Configure 'Do not allow drive redirection' (Not Scored) 274
1.2.3.4.2.2 Connections 275
1.2.3.4.2.2.1 Configure 'Allow users to connect remotely using Remote Desktop Services' (Not Scored) 275
1.2.3.4.2.3 Security 276
1.2.3.4.2.3.1 Configure 'Set client connection encryption level' (Not Scored) 276

1.2.3.4.2.3.2 Configure 'Always prompt for password upon connection' (Not Scored) 277
1.2.3.5 Windows Error Reporting 278
1.2.3.5.1 Advanced Error Reporting Settings 279
1.2.3.5.1.1 Configure 'Report operating system errors' (Not Scored) 279
1.2.3.5.2 Configure 'Display Error Notification' (Not Scored) 280
1.2.3.6 NetMeeting 281
1.2.3.6.1 Configure 'Disable remote Desktop Sharing' (Not Scored) 281
1.2.3.7 Windows Installer 282
1.2.3.7.1 Set 'Always install with elevated privileges' to 'Disabled' (Scored) 282
1.2.3.8 Credential User Interface 284
1.2.3.8.1 Configure 'Require trusted path for credential entry.' (Not Scored) 284
Appendix: Change History 286

Overview

This document, CIS Microsoft Windows Server 2003 Benchmark v3.0.0, provides prescriptive guidance for establishing a secure configuration posture for CIS Microsoft Windows Server 2003. To obtain the latest version of this guide, please visit http://benchmarks.cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Intended Audience

This document is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Microsoft Windows Server 2003.

Consensus Guidance

This benchmark was created using a consensus review process comprised 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://community.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 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.

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.

Microsoft's Security Compliance Management Toolkit was an excellent resource in the development of this Benchmark. CIS also extends special recognition to the development teams of those resources. Readers are encouraged to download the toolkit to access many great resources, including tools such as GPOAccelerator and DCM Configuration Packs, which aid in the rapid deployment of security configuration policies

Recommendations

1 Computer Configuration

1.1 Windows Settings

1.1.1 Security Settings

1.1.1.1 Account Policies

1.1.1.1.1 Kerberos Policy

1.1.1.1.1.1 Configure 'Maximum lifetime for service ticket' (Not Scored)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This security setting determines the maximum amount of time (in minutes) that a granted session ticket can be used to access a particular service. The setting must be greater than 10 minutes and less than or equal to the setting for Maximum lifetime for user ticket. If a client presents an expired session ticket when it requests a connection to a server, the server returns an error message. The client must request a new session ticket from the Kerberos V5 Key Distribution Center (KDC). Once a connection is authenticated, however, it no longer matters whether the session ticket remains valid. Session tickets are used only to authenticate new connections with servers. Ongoing operations are not interrupted if the session ticket that is used to authenticate the connection expires during the connection. Default: 600 minutes (10 hours).

Rationale:

If you configure the value for the Maximum lifetime for service ticket setting too high, then users might be able to access network resources outside of their logon hours. Also, users

whose accounts were disabled might have continued access to network services with valid service tickets that were issued before their accounts were disabled.

Audit:

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

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

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

Impact:

None. This is the default configuration.

1.1.1.1.1.2 Configure 'Enforce user logon restrictions' (Not Scored)

Profile Applicability:

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

Description:

Kerberos policy settings determine Kerberos-related attributes of domain user accounts, such as the Maximum lifetime for user ticket and Enforce user logon restrictions settings. However, these policy settings are not used for stand-alone client computers because they do not participate in a domain.

Rationale:

If you disable this policy setting, users could receive session tickets for services that they no longer have the right to use because the right was removed after they logged on.

Audit:

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

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

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

Impact:

None. This is the default configuration.

1.1.1.1.1.3 Configure 'Maximum lifetime for user ticket' (Not Scored)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This security setting determines the maximum amount of time (in hours) that a user's ticket-granting ticket (TGT) may be used. When a user's TGT expires, a new one must be requested or the existing one must be renewed. Default: 10 hours.

Rationale:

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

Audit:

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

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

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

Impact:

Reducing this setting from the default value reduces the likelihood that the TGT will be used to access resources that the user does not have rights to. However, it will require

more frequent requests to the KDC for TGTs on behalf of users. Most KDCs can support a value of four hours without too much additional burden.

1.1.1.1.1.4 Configure 'Maximum tolerance for computer clock synchronization' (Not Scored)

Profile Applicability:

- Level 1 - Domain Controller

Description:

Many security services, especially authentication, rely on an accurate computer clock to perform their jobs. You should ensure computer time is accurate and that all servers in your organization use the same time source. The Windows Server 2003 W32Time service provides time synchronization for Windows Server 2003 and Microsoft Windows XP based computers that run in an Active Directory domain. The W32Time service synchronizes the clocks of Windows Server 2003based computers with the domain controllers in a domain. This synchronization is necessary for the Kerberos protocol and other authentication protocols to work properly. To function correctly, a number of Windows Server family components rely on accurate and synchronized time. If the clocks are not synchronized on the clients, the Kerberos authentication protocol might deny access to users. Another important benefit that time synchronization provides is event correlation on all of the clients in your enterprise. Synchronized clocks on the clients in your environment ensure that you can correctly analyze events that take place in uniform sequence on those clients throughout the organization. The W32Time service uses the Network Time Protocol (NTP) to synchronize clocks on computers that run Windows Server 2003. In a Windows Server 2003 forest, time is synchronized by default in the following manner: . The primary domain controller (PDC) emulator operations master in the forest root domain is the authoritative time source for the organization. . All PDC operation masters in other domains in the forest follow the hierarchy of domains when they select a PDC emulator with which to synchronize their time. . All domain controllers in a domain synchronize their time with the PDC emulator operations master in their domain as their inbound time partner. . All member servers and client desktop computers use the authenticating domain controller as their inbound time partner. To ensure that the time is accurate, the PDC emulator in the forest root domain can be synchronized to an authoritative time source, such as a reliable NTP source or a highly accurate clock on your network. Note that NTP synchronization uses UDP port 123 traffic. Before you synchronize with an external server, you should weigh the benefits of opening this port against the potential security risk. Also, if you synchronize with an external server that you do not control, you risk configuring your servers with the incorrect time. The external server could be compromised or spoofed by

an attacker to maliciously manipulate the clocks on your computers. As explained earlier, the Kerberos authentication protocol requires synchronized computer clocks. If they are not synchronized, a denial of service may occur.

Rationale:

To prevent "replay attacks," the Kerberos authentication protocol uses time stamps as part of its protocol definition. For time stamps to work properly, the clocks of the client and the domain controller need to be closely synchronized. Because the clocks of two computers are often not synchronized, administrators can use this policy to establish the maximum acceptable difference to Kerberos between a client clock and a domain controller clock. If the difference between the client clock and the domain controller clock is less than the maximum time difference specified in this setting, any time stamp that is used in a session between the two computers is considered to be authentic.

Audit:

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

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

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

Impact:

None. This is the default configuration.

1.1.1.1.1.5 Configure 'Maximum lifetime for user ticket renewal' (Not Scored)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This policy setting determines the period of time (in days) during which a user's ticket-granting ticket (TGT) can be renewed. To prevent replay attacks, the Kerberos authentication protocol uses time stamps as part of its protocol definition. For time stamps to work properly, the clocks of the client and the domain controller need to be

synchronized as closely as possible. Because the clocks of two computers are often not synchronized, administrators can use this policy to establish the maximum elapsed time within which a Kerberos negotiation must complete; the elapsed time is computed from the timestamps. The value of this setting limits the maximum time difference that can be tolerated between the domain controller and the client computer.

Rationale:

If the value for the Maximum lifetime for user ticket renewal setting is too high, users might be able to renew very old user tickets.

Audit:

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

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

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

Impact:

None. This is the default configuration.

1.1.1.2 Local Policies

1.1.1.2.1 Security Options

1.1.1.2.1.1 Set 'Domain controller: Allow server operators to schedule tasks' to 'Disabled' (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.

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 object is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa:SubmitControl
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `0`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Domain controller: Allow server operators to schedule tasks
```

Impact:

The impact 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. However, those jobs will run in the context of the account that the user authenticates with when setting up the job.

1.1.1.2.1.2 Configure 'Domain controller: Allow server operators to schedule tasks' (Not Scored)

Profile Applicability:

- Level 1 - Member Server

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.

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 for your organization. This group policy object is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa:SubmitControl
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Domain controller: Allow server operators to schedule tasks
```

Impact:

The impact 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. However, those jobs will run in the context of the account that the user authenticates with when setting up the job.

1.1.1.2.1.3 Set 'Accounts: Guest account status' to 'Disabled' (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. Note that this setting will have no impact when applied to the domain controller 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 implement the recommended configuration state, set the following Group Policy setting to `0`.

```
Computer Configuration\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 later versions of Windows.

1.1.1.2.1.4 Set 'Accounts: Limit local account use of blank passwords to console logon only' 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.

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 Windows Server 2003 Active Directory® directory service 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 object is backed by the following registry location:

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

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `1`.

```
Computer Configuration\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 configuration.

1.1.1.2.1.5 Set 'Domain controller: Refuse machine account password changes' to 'Disabled' (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. By default, member computers change their computer account passwords every 30 days. If enabled, the domain controller will refuse computer account password change requests. If it is enabled, this setting does not allow a domain controller to accept any changes to a computer account's password. Default: This policy is not defined, which means that the system treats it as Disabled.

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 object is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters:RefusePasswor
dChange
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `0`.

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

Impact:

None. This is the default configuration.

1.1.1.2.1.6 Configure 'Domain controller: Refuse machine account password changes' (Not Scored)

Profile Applicability:

- Level 1 - Member Server

Description:

This security setting determines whether domain controllers will refuse requests from member computers to change computer account passwords. By default, member computers change their computer account passwords every 30 days. If enabled, the domain controller will refuse computer account password change requests. If it is enabled, this setting does not allow a domain controller to accept any changes to a computer account's password. Default: This policy is not defined, which means that the system treats it as Disabled.

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 for your organization. This group policy object is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters:RefusePasswor
dChange
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

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

Impact:

None. This is the default configuration.

1.1.1.2.1.7 Set 'Accounts: Administrator account status' to 'Disabled' (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 controller 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:

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 implement the recommended configuration state, set the following Group Policy setting to `0`.

```
Computer Configuration\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.

1.1.1.2.1.8 Set 'System objects: Default owner for objects created by members of the Administrators group' to 'Object creator' (Scored)

Profile Applicability:

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

Description:

This policy setting determines whether the Administrators group or an object creator is the default owner of any system objects that are created. When system objects are created, the ownership will reflect which account created the object rather than the more generic Administrators group.

Rationale:

If you configure this policy setting to Administrators group, it will be impossible to hold individuals accountable for the creation of new system objects.

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\System\CurrentControlSet\Control\Lsa:nodefaultadminowner
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `1`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\System objects: Default owner for objects created by members of the
Administrators group
```

Impact:

When system objects are created, the ownership will reflect which account created the object instead of the more generic Administrators group. A consequence of this policy setting is that objects will become orphaned when user accounts are deleted. For example, when a member of the information technology group leaves, any objects that they created anywhere in the domain will have no owner. This situation could become an administrative burden as administrators have to manually take ownership of orphaned objects to update their permissions. This potential burden can be minimized if you can ensure that Full Control is always assigned to new objects for a domain group such as Domain Admins.

1.1.1.2.1.9 Set 'Network access: Shares that can be accessed anonymously' to '' (Scored)

Profile Applicability:

- Level 1 - Domain Controller

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. Note: It can be very dangerous to add other shares to this Group Policy setting. Any network user can access any shares that are listed, which could exposure or corrupt sensitive data. Note: 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.

Rationale:

It is very dangerous to enable 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 object is backed by the following registry location:

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

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to .

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

Impact:

There should be little impact because this is the default configuration. Only authenticated users will have access to shared resources on the server.

1.1.1.2.1.10 Set 'Network access: Shares that can be accessed anonymously' to 'None' (Scored)

Profile Applicability:

- 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. Note: It can be very dangerous to add other shares to this Group Policy setting. Any network user can access any shares that are listed, which could exposure or corrupt sensitive data. Note: 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.

Rationale:

It is very dangerous to enable 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 object is backed by the following registry location:

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

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `None`.

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

Impact:

There should be little impact because this is the default configuration. Only authenticated users will have access to shared resources on the server.

1.1.1.2.1.11 Set 'Interactive logon: Smart card removal behavior' to 'Lock Workstation' (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.

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. This group policy object is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon:scremoveoption
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `1`.

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

Impact:

If you select Force Logoff, users will have to re-insert their smart cards and re-enter their PINs when they return to their workstations. 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.

1.1.1.2.1.12 Set 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' to 'Require message integrity,Require message confidentiality,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 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 possible values for the Network security: Minimum session security for NTLM SSP based (including secure RPC) clients setting are: . Require message confidentiality. This option is only available in Windows XP and Windows Server 2003, the connection will fail if encryption is not negotiated. Encryption converts data into a form that is not readable until

decrypted. . Require message integrity. This option is only available in Windows XP and Windows Server 2003, the connection will fail if message integrity is not negotiated. The integrity of a message can be assessed through message signing. Message signing proves that the message has not been tampered with; it attaches a cryptographic signature that identifies the sender and is a numeric representation of the contents of the message. . Require 128-bit encryption. The connection will fail if strong encryption (128-bit) is not negotiated. . Require NTLMv2 session security. The connection will fail if the NTLMv2 protocol is not negotiated. . Not Defined.

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. 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 object is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0:NTLMMinClientSec
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `537395248`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Network security: Minimum session security for NTLM SSP based (including
secure RPC) clients
```

Impact:

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 "How to apply more restrictive security settings on a Windows Server 2003-based cluster server" at http://support.microsoft.com/default.aspx?scid=kb;en-us;891597 and "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" at http://support.microsoft.com/kb/890761/ for more information on possible issues and how to resolve them.

1.1.1.2.1.13 Set 'Devices: Prevent users from installing printer drivers' to 'Enabled' (Scored)

Profile Applicability:

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

Description:

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. To reduce the possibility of such an event, only administrators should be allowed to install printer drivers. However, because laptops are mobile devices, laptop users may occasionally need to install a printer driver from a remote source to continue their work. Therefore, this policy setting should be disabled for laptop users, but always enabled for desktop users.

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.

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\System\CurrentControlSet\Control\Print\Providers\LanMan Print
Services\Servers:AddPrinterDrivers
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `1`.

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

Impact:

Only users with Administrative, Power User, or Server Operator privileges will be able to install printers on the servers. If this policy setting is enabled but the driver for a network printer already exists on the local computer, users can still add the network printer.

1.1.1.2.1.14 Set 'Devices: Unsigned driver installation behavior' to 'Warn but allow installation' (Scored)

Profile Applicability:

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

Description:

This policy setting determines what happens when an attempt is made to install a device driver (by means of Setup API) that has not been approved and signed by the Windows Hardware Quality Lab (WHQL). Depending on how you configure it, this policy setting will prevent the installation of unsigned drivers or warn the administrator that an unsigned driver is about to be installed. The Devices: Unsigned driver installation behavior setting can be used to prevent the installation of drivers that have not been certified to run on Windows Server 2003 with SP1. One potential problem with this configuration is that unattended installation scripts will fail when they attempt to install unsigned drivers.

Rationale:

This policy setting will not prevent a method that is used by some attack tools in which malicious .sys files are copied and registered to start as system services.

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\Microsoft\Driver Signing:Policy
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `01`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Devices: Unsigned driver installation behavior
```

Impact:

Users with sufficient privileges to install device drivers will be able to install unsigned device drivers. However, this capability could result in stability problems for servers. Another potential problem with a Warn but allow installation configuration is that unattended installation scripts will fail if they attempt to install unsigned drivers.

1.1.1.2.1.15 Set 'Recovery console: Allow floppy copy and access to all drives and all folders' to 'Disabled' (Scored)

Profile Applicability:

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

Description:

This policy setting makes the Recovery Console SET command available, which allows you to set the following recovery console environment variables: . AllowWildCards. Enables wildcard support for some commands (such as the DEL command). . AllowAllPaths. Allows access to all files and folders on the computer. . AllowRemovableMedia. Allows files to be copied to removable media, such as a floppy disk. . NoCopyPrompt. Does not prompt when overwriting an existing file.

Rationale:

An attacker who can cause the system to restart into the Recovery Console could steal sensitive data and leave no audit or access trail.

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\Microsoft\Windows
NT\CurrentVersion\Setup\RecoveryConsole:setcommand
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `0`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Recovery console: Allow floppy copy and access to all drives and all folders
```

Impact:

Users who have started a server through the Recovery Console and logged in with the built-in Administrator account will not be able to copy files and folders to a floppy disk.

1.1.1.2.1.16 Set 'MSS: (DisableSavePassword) Prevent the dial-up password from being saved (recommended)' to 'Enabled' (Scored)

Profile Applicability:

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

Description:

This entry appears as MSS: (DisableSavePassword) Prevent the dial-up password from being saved (recommended) in the SCE. By default, Windows will offer the option to save passwords for dial-up and VPN connections, which is not desirable on a server. You can add this registry value to the template file in the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\ Parameters\ subkey.

Rationale:

An attacker who steals a mobile user's computer could automatically connect to the organization's network if the Save This Password check box is enabled for the dial-up entry.

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\SYSTEM\CurrentControlSet\Services\RasMan\Parameters:DisableSavePass
word
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `1`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\MSS: (DisableSavePassword) Prevent the dial-up password from being saved
(recommended)
```

Impact:

Users won't be able to automatically store their logon credentials for dial-up and VPN connections.

1.1.1.2.1.17 Set 'Network access: Restrict anonymous access to Named Pipes and Shares' 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 HKLM\System \CurrentControlSet\Services\LanManServer\Parameters registry key. This registry value toggles null session shares on or off to control whether the server service restricts unauthenticated clients' access to named resources. Null sessions are a weakness that can be exploited through shares (including the default shares) on computers in your environment.

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 object is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters:restrictn
ullsessaccess
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `1`.

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

Impact:

You can enable this policy setting to restrict null session access for unauthenticated users to all server pipes and shared folders except those that are listed in the NullSessionPipes and NullSessionShares entries. 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 setting. Previous to the release of Windows Server 2003 with Service Pack 1 (SP1) some named pipes were allowed anonymous access by default, but with the increased hardening in Windows Server 2003 with SP1 more pipes must be explicitly added if needed.

1.1.1.2.1.18 Set 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' to '90' (Scored)

Profile Applicability:

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

Description:

The registry value entry WarningLevel was added to the template file in the HKEY_LOCAL_MACHINE\ SYSTEM\CurrentControlSet\Services\Eventlog\Security\ registry key. The entry appears as MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning in the SCE. This setting can generate a security audit in the Security event log when the log reaches a user-defined threshold. 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 object is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security:WarningLevel
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `90`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\MSS: (WarningLevel) Percentage threshold for the security event log at which
the system will generate a warning
```

Impact:

This setting will generate an audit event when the Security log reaches the 90 percent-full threshold unless the log is configured to overwrite events as needed.

1.1.1.2.1.19 Set 'MSS: (SynAttackProtect) Syn attack protection level (protects against DoS)' to 'Connections time out sooner if a SYN attack is detected' (Scored)

Profile Applicability:

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

Description:

This entry appears as MSS: (SynAttackProtect) Syn attack protection level (protects against DoS) in the SCE. This entry causes TCP to adjust retransmission of SYN-ACKs. When you configure this entry, the overhead of incomplete transmissions in a connect request (SYN) attack is reduced. You can use this entry to configure Windows to send router discovery messages as broadcasts instead of multicasts, as described in RFC 1256. By default, if router discovery is enabled, router discovery solicitations are sent to the all-routers multicast group (224.0.0.2). Not applicable to Windows Vista or Windows Server 2008.

Rationale:

In a SYN flood attack, the attacker sends a continuous stream of SYN packets to a server. The server leaves the half-open connections open until it is overwhelmed and is no longer able to respond to legitimate requests

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\System\CurrentControlSet\Services\Tcpip\Parameters:SynAttackProtect
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `1`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\MSS: (SynAttackProtect) Syn attack protection level (protects against DoS)
```

Impact:

This value adds more delays to connection indications, and TCP connection requests quickly time out when a SYN attack is in progress. If you configure this registry entry, the scalable windows and TCP parameters that are configured on each adapter (including Initial Round Trip Time (RTT) and window size), socket options no longer work. When the computer is attacked, the scalable windows (RFC 1323) and per adapter configured TCP parameters (Initial RTT, window size) options on any socket can no longer be enabled. The reasons these options cannot be enabled is because when protection is functioning, the route cache entry is not queried before the SYN-ACK is sent and the Winsock options are not available at this stage of the connection.

1.1.1.2.1.20 Set 'System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies' to 'Enabled' (Scored)

Profile Applicability:

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

Description:

This policy setting determines whether digital certificates are processed when software restriction policies are enabled and a user or process attempts to run software with an .exe file name extension. It enables or disables certificate rules (a type of software restriction policies rule). With software restriction policies, you can create a certificate rule that will allow or disallow the execution of Authenticode®-signed software, based on the digital certificate that is associated with the software. For certificate rules to take effect in software restriction policies, you must enable this policy setting.

Rationale:

Software restriction policies help to protect users and computers because they can prevent the execution of unauthorized code, such as viruses and Trojans horses.

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\Safer\CodeIdentifiers:AuthenticodeEnabled
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `1`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies
```

Impact:

If you enable certificate rules, software restriction policies check a certificate revocation list (CRL) to ensure that the software's certificate and signature are valid. This checking process may negatively affect performance when signed programs start. To disable this feature you can edit the software restriction policies in the desired GPO. On the Trusted Publishers Properties dialog box, clear the Publisher and Timestamp check boxes.

1.1.1.2.1.21 Set 'MSS: (AutoShareServer) Enable Administrative Shares (recommended except for highly secure environments)' to 'Enabled' (Scored)

Profile Applicability:

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

Description:

This entry appears as MSS: (AutoShareServer) Enable Administrative Shares (not recommended except for highly secure environments) in the SCE. For additional information, see the Microsoft Knowledge Base article How to remove administrative shares in Windows Server 2008 at http://support.microsoft.com/kb/954422/en-us.

Rationale:

Because these built-in administrative shares are well-known and present on most Windows computers, malicious users often target them for brute-force attacks to guess passwords as well as other types of attacks.

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\System\CurrentControlSet\Services\LanmanServer\Parameters:AutoShare
Server
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `1`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\MSS: (AutoShareServer) Enable Administrative Shares (recommended except for
highly secure environments)
```

Impact:

If you delete these shares you could cause problems for administrators and programs or services that rely on these shares. For example, both Microsoft Systems Management Server (SMS) and Microsoft Operations Manager require administrative shares for correct installation and operation. Also, many third-party network backup applications require administrative shares.

1.1.1.2.1.22 Set 'Shutdown: Clear virtual memory pagefile' to 'Disabled' (Scored)

Profile Applicability:

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

Description:

This policy setting determines whether the virtual memory pagefile is cleared when the system is shut down. When this policy setting is enabled, the system pagefile is cleared each time that the system shuts down properly. If you enable this security setting, the hibernation file (Hiberfil.sys) is zeroed out when hibernation is disabled on a portable computer system. It will take longer to shut down and restart the computer, and will be especially noticeable on computers with large paging files.

Rationale:

Important information that is kept in real memory may be written periodically to the page file to help Windows handle multitasking functions. An attacker who has physical access to a server that has been shut down could view the contents of the paging file. The attacker could move the system volume into a different computer and then analyze the contents of the paging file. Although this process is time consuming, it could expose data that is cached from random access memory (RAM) to the paging file. Caution: An attacker who has physical access to the server could bypass this countermeasure by simply unplugging the server from its power source.

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\System\CurrentControlSet\Control\Session Manager\Memory
Management:ClearPageFileAtShutdown
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `0`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Shutdown: Clear virtual memory pagefile
```

Impact:

It will take longer to shut down and restart the server, especially on servers with large paging files. For a server with 2 gigabytes (GB) of RAM and a 2-GB paging file, this policy setting could increase the shutdown process by 20 to 30 minutes, or more. For some organizations, this downtime violates their internal service level agreements. Therefore, use caution before you implement this countermeasure in your environment.

1.1.1.2.1.23 Set 'Domain member: Disable machine account password changes' 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. If you enable this policy setting, the domain member will be prevented from changing its computer account password. If you disable this policy setting, the domain member can change its computer account password as specified by the Domain Member: Maximum machine account password age setting, which by default is every 30 days. 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.

Rationale:

The default configuration 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 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 object is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters:disablepasswo
rdchange
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `0`.

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

Impact:

None. This is the default configuration.

1.1.1.2.1.24 Set 'Microsoft network server: Amount of idle time required before suspending session' to '15' (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. A value of 0 will disconnect an idle session as quickly as possible. The maximum value is 99999, which is 208 days; in effect, this value disables the setting.

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 object is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters:autodisco
nnect
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `15`.

```
Computer Configuration\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.

1.1.1.2.1.25 Set 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' to 'Enabled' (Scored)

Profile Applicability:

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

Description:

The registry value entry NoNameReleaseOnDemand was added to the template file in the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netbt\ Parameters\ registry key. The entry appears as MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers in the SCE. 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.

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. 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. For more information, see the Microsoft Knowledge Base article "MS00-047: NetBIOS Vulnerability May Cause Duplicate Name on the Network Conflicts" at http://support.microsoft.com/default.aspx?kbid=269239.

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\System\CurrentControlSet\Services\Netbt\Parameters:NoNameReleaseOnDemand
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `1`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers
```

Impact:

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.

1.1.1.2.1.26 Configure 'Devices: Restrict CD-ROM access to locally logged-on user only' (Not Scored)

Profile Applicability:

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

Description:

This policy setting determines whether a CD-ROM is accessible to both local and remote users simultaneously. If you enable this policy setting, only the interactively logged-on user is allowed to access removable CD-ROM media. When this policy setting is enabled and no one is logged on interactively, the CD-ROM is accessible over the network.

Rationale:

A remote user could potentially access a mounted CD that contains sensitive information. This risk is small, because CD drives are not automatically made available as shared drives; administrators must deliberately choose to share the drive. However, administrators may wish to deny network users the ability to view data or run applications from removable media on the server.

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\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon:AllocateCDRoms
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Devices: Restrict CD-ROM access to locally logged-on user only
```

Impact:

Users who connect to the server over the network will not be able to use any CD drives that are installed on the server whenever anyone is logged on to the local console of the server. System tools that require access to the CD drive will fail. For example, the Volume Shadow Copy service attempts to access all CD and floppy disk drives that are present on the computer when it initializes, and if the service cannot access one of these drives, it will fail. This condition will cause the Windows Backup tool to fail if volume shadow copies were specified for the backup job. Any non-Microsoft backup products that use volume shadow copies will also fail. This policy setting would not be suitable for a computer that serves as a CD jukebox for network users.

1.1.1.2.1.27 Set 'MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds' to '300000 or 5 minutes (recommended)' (Scored)

Profile Applicability:

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

Description:

The registry value entry KeepAliveTime was added to the template file in the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\ registry key. The entry appears as MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds (300,000 is recommended) in the SCE. 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.

Rationale:

An attacker who is able to connect to network applications could establish numerous connections to cause a denial of service (DoS) condition.

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\System\CurrentControlSet\Services\Tcpip\Parameters:KeepAliveTime
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `300000`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds
```

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.

1.1.1.2.1.28 Set 'Shutdown: Allow system to be shut down without having to log on' 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.

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 denial of service (DoS) condition. Attackers could also shut down the server and leave all of its applications and services unavailable.

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\Microsoft\Windows\CurrentVersion\Policies\System:ShutdownW
ithoutLogon
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `0`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Shutdown: Allow system to be shut down without having to log on
```

Impact:

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

1.1.1.2.1.29 Set 'Interactive logon: Do not display last user name' 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.

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 Terminal 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 object is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System:DontDispl
ayLastUserName
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `1`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Interactive logon: Do not display last user name
```

Impact:

Users will not see their user name or domain name when unlocking their computer, they will have to enter that information.

1.1.1.2.1.30 Set 'Network security: LAN Manager authentication level' to 'Send NTLMv2 response only. Refuse LM & NTLM' (Scored)

Profile Applicability:

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

Description:

LAN Manager (LM) is a family of early Microsoft client/server software that allows users to link personal computers together on a single network. Network capabilities include 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 possible values for the Network security: LAN Manager authentication level setting are: . Send LM & NTLM responses . Send LM & NTLM use NTLMv2 session security if negotiated . Send NTLM responses only . Send NTLMv2 responses only . Send NTLMv2 responses only\refuse LM . Send NTLMv2 responses only\refuse LM & NTLM . Not Defined The Network security: LAN Manager authentication level setting determines which challenge/response authentication protocol is used for network logons. This choice affects the authentication protocol level that clients use, the session security level that the computers negotiate, and the authentication level that servers accept as follows: . Send LM & NTLM responses. Clients use LM and NTLM authentication and never use NTLMv2 session security. Domain controllers accept LM, NTLM, and NTLMv2 authentication. . Send LM & NTLM use NTLMv2 session security if negotiated. Clients use LM and NTLM authentication and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication. . Send NTLM response only. Clients use NTLM authentication only and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication. . Send NTLMv2 response only. Clients use NTLMv2 authentication only and

use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication. . Send NTLMv2 response only\refuse LM. Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it. Domain controllers refuse LM (accept only NTLM and NTLMv2 authentication). . Send NTLMv2 response only\refuse LM & NTLM. 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). These settings correspond to the levels discussed in other Microsoft documents as follows: . Level 0 Send LM and NTLM response; never use NTLMv2 session security. Clients use LM and NTLM authentication, and never use NTLMv2 session security. Domain controllers accept LM, NTLM, and NTLMv2 authentication. . Level 1 Use NTLMv2 session security if negotiated. Clients use LM and NTLM authentication, and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication. . Level 2 Send NTLM response only. Clients use only NTLM authentication, and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication. . Level 3 Send NTLMv2 response only. Clients use NTLMv2 authentication, and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication. . Level 4 Domain controllers refuse LM responses. Clients use NTLM authentication, and use NTLMv2 session security if the server supports it. Domain controllers refuse LM authentication, that is, they accept NTLM and NTLMv2. . Level 5 Domain controllers refuse LM and NTLM responses (accept only NTLMv2). Clients use NTLMv2 authentication, use and NTLMv2 session security if the server supports it. Domain controllers refuse NTLM and LM authentication (they accept only NTLMv2).

Rationale:

In Windows Vista, this setting is undefined. However, in Windows 2000, Windows Server 2003, and Windows XP clients are configured by default to send LM and NTLM authentication responses (Windows 95-based and Windows 98-based clients only send LM). The default setting on servers allows all clients to authenticate with servers and use their resources. However, this means that LM responses the weakest form of authentication response are sent over the network, and it is 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 earlier 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 domain controllers.

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\System\CurrentControlSet\Control\Lsa:LmCompatibilityLevel
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to 5.

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

Impact:

Clients that do not support NTLMv2 authentication will not be able to authenticate in the domain and access domain resources by using LM and NTLM. Note: For information about a hotfix to ensure that this setting works in networks that include Windows NT 4.0-based computers along with Windows 2000, Windows XP, and Windows Server 2003-based computers, see article 305379, Authentication Problems in Windows 2000 with NTLM 2 Levels Above 2 in a Windows NT 4.0 Domain, in the Microsoft Knowledge Base (http://go.microsoft.com/fwlink/?LinkId=100907).

1.1.1.2.1.31 Configure 'DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax' (Not Scored)

Profile Applicability:

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

Description:

This policy setting determines which users or groups might access DCOM application remotely or locally. This setting is used to control the attack surface of the computer for DCOM applications. You can use this policy setting to specify access permissions to all the computers to particular users for DCOM applications in the enterprise. When you specify the users or groups that are to be given permission, the security descriptor field is populated with the Security Descriptor Definition Language representation of those groups

and privileges. If the security descriptor is left blank, the policy setting is defined in the template, but it is not enforced. Users and groups can be given explicit Allow or Deny privileges on both local access and remote access. The registry settings that are created as a result of enabling the DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax policy setting take precedence over (have higher priority) the previous registry settings in this area. RpcSs checks the new registry keys in the Policies section for the computer restrictions, and these registry entries take precedence over the existing registry keys under OLE. This means that previously existing registry settings are no longer effective, and if you make changes to the existing settings, the computer access permissions for any users are not changed. You should take care to correctly configure their list of users and groups. The possible values for this policy setting are: Blank. This represents the local security policy way of deleting the policy enforcement key. This value deletes the policy and then sets it as Not defined state. The Blank value is set by using the ACL editor and emptying the list, and then pressing OK. SDDL. This is the Security Descriptor Definition Language representation of the groups and privileges you specify when you enable this policy. Not Defined. This is the default value. Note If the administrator is denied permission to access DCOM applications due to the changes made to DCOM in SP2, the administrator can use the DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax policy setting to manage DCOM access to the computer. The administrator can specify which users and groups can access the DCOM application on the computer both locally and remotely by using this setting. This will restore control of the DCOM application to the administrator and users. To do this, open the DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax setting, and click Edit Security. Specify the groups you want to include and the computer access permissions for those groups. This defines the setting and sets the appropriate SDDL value.

Rationale:

Many COM applications include some security-specific code (for example, to call CoInitializeSecurity) but use weak settings that often allow unauthenticated access to the process. Administrators cannot override these settings to force stronger security in earlier versions of Windows without modifying the application. An attacker could attempt to exploit weak security in an individual application by attacking it through COM calls. Also, COM infrastructure includes the Remote Procedure Call System Service (RPCSS), a system service that runs during computer startup and always runs after that. This service manages activation of COM objects and the running object table, and provides helper services to DCOM remoting. It exposes RPC interfaces that can be called remotely. Because some COM servers allow unauthenticated remote access, these interfaces can be called by anyone,

including unauthenticated users. As a result, RPCSS can be attacked by malicious users who use remote, unauthenticated computers.

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\Software\policies\Microsoft\windows
NT\DCOM:MachineAccessRestriction
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\DCOM: Machine Access Restrictions in Security Descriptor Definition Language
(SDDL) syntax
```

Impact:

Windows operating systems implement default COM ACLs when they are installed. Modifying these ACLs from the default may cause some applications or components that communicate by using DCOM to fail. If you implement a COM server and you override the default security settings, confirm that the application-specific call permissions ACL assigns correct permission to appropriate users. If it does not, you need to change your application-specific permission ACL to provide appropriate users with activation rights so that applications and Windows components that use DCOM do not fail.

1.1.1.2.1.32 Configure 'MSS: (Hidden) Hide Computer From the Browse List (not recommended except for highly secure environments)' (Not Scored)

Profile Applicability:

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

Description:

The registry value entry Hidden was added to the template file in the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Lanmanserver\Parameters\ registry key. The entry appears as MSS: (Hidden) Hide Computer From the Browse List (not

recommended except for highly secure environments) in the SCE. You can configure a computer so that it does not send announcements to browsers on the domain. If you do so, you hide the computer from the Browse list, which means that the computer will stop announcing itself to other computers on the same network. An attacker who knows the name of a computer can more easily gather additional information about the system. You can enable this setting to remove one method that an attacker might use to gather information about computers on the network. Also, this setting can help reduce network traffic when enabled. However, the security benefits of this setting are small because attackers can use alternative methods to identify and locate potential targets. For this reason, Microsoft recommends to configure this setting to Enabled in high security environments, and to configure it to Not Defined in enterprise environments. For additional information, see the Knowledge Base article 321710, HOW TO: Hide a Windows 2000-Based Computer from the Browser List.

Rationale:

An attacker who knows the name of a computer can more easily gather additional information about the computer. If you enable this entry, you remove one method that an attacker might use to gather information about computers on the network. Also, if you enable this entry you can help reduce network traffic. However, the vulnerability is small because attackers can use alternative methods to identify and locate potential targets.

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\Lanmanserver\Parameters:Hidden
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\MSS: (Hidden) Hide Computer From the Browse List (not recommended except for
highly secure environments)
```

Impact:

The computer will no longer appear on the Browser list or in Network Neighborhood on other computers on the same network.

1.1.1.2.1.33 Set 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' to 'Disabled' (Scored)

Profile Applicability:

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

Description:

The registry value entry AutoAdminLogon was added to the template file in the HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ registry key. The entry appears as MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended) in the Security Configuration Editor. 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 the Knowledge Base article 315231, How to turn on automatic logon in Windows XP.

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 object is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon:AutoAdminLogon
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `0`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)
```

Impact:

None. By default this entry is not enabled.

1.1.1.2.1.34 Set 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' to 'Require message integrity,Require message confidentiality,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 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 possible values for the Network security: Minimum session security for NTLM SSP based (including secure RPC) servers setting are: . Require message confidentiality. This option is only available in Windows XP and Windows Server 2003, the connection will fail if encryption is not negotiated. Encryption converts data into a form that is not readable until decrypted. . Require message integrity. This option is only available in Windows XP and Windows Server 2003, the connection will fail if message integrity is not negotiated. The integrity of a message can be assessed through message signing. Message signing proves that the message has not been tampered with; it attaches a cryptographic signature that identifies the sender and is a numeric representation of the contents of the message. . Require 128-bit encryption. The connection will fail if strong encryption (128-bit) is not negotiated. . Require NTLMv2 session security. The connection will fail if the NTLMv2 protocol is not negotiated. . Not Defined.

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 object is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0:NTLMMinServerSec
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `537395248`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Network security: Minimum session security for NTLM SSP based (including
secure RPC) servers
```

Impact:

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 "How to apply more restrictive security settings on a Windows Server 2003-based cluster server" at http://support.microsoft.com/default.aspx?scid=kb;en-us;891597 and "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" at http://support.microsoft.com/kb/890761/ for more information on possible issues and how to resolve them.

1.1.1.2.1.35 Set 'System objects: Require case insensitivity for non-Windows subsystems' 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.

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 object is backed by the following registry location:

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

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `1`.

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

Impact:

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.

1.1.1.2.1.36 Configure 'DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax' (Not Scored)

Profile Applicability:

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

Description:

This policy setting determines which users or groups might launch or activate DCOM applications remotely or locally. This setting is used to control the attack surface of the

computer for DCOM applications. You can use this Group Policy setting to grant access to all the computers to particular users for DCOM application in the enterprise. When you define this setting, and specify the users or groups that are to be given permission, the security descriptor field is populated with the Security Descriptor Definition Language representation of those groups and privileges. If the security descriptor is left blank, the policy setting is defined in the template, but it is not enforced. Users and groups can be given explicit Allow or Deny privileges on local launch, remote launch, local activation, and remote activation. The registry settings that are created as a result of this policy take precedence over the previous registry settings in this area. RpcSs checks the new registry keys in the Policies section for the computer restrictions; these entries take precedence over the existing registry keys under OLE. The possible values for this Group Policy setting are: Blank. This represents the local security policy way of deleting the policy enforcement key. This value deletes the policy and then sets it to Not defined state. The Blank value is set by using the ACL editor and emptying the list, and then pressing OK. SDDL. This is the Security Descriptor Definition Language representation of the groups and privileges you specify when you enable this policy. Not Defined. This is the default value. Note If the administrator is denied access to activate and launch DCOM applications due to the changes made to DCOM in SP2, this policy setting can be used for controlling the DCOM activation and launch to the computer. The administrator can specify which users and groups can launch and activate DCOM applications on the computer both locally and remotely by using the DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax policy setting. This restores control of the DCOM application to the administrator and specified users. To do this, open the DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax setting, and click Edit Security. Specify the groups you want to include and the computer launch permissions for those groups. This defines the setting and sets the appropriate SDDL value.

Rationale:

Many COM applications include some security-specific code (for example, to call CoInitializeSecurity) but use weak settings that often allow unauthenticated access to the process. Administrators cannot override these settings to force stronger security in earlier versions of Windows without modifying the application. An attacker could attempt to exploit weak security in an individual application by attacking it through COM calls. Also, COM infrastructure includes the RPCSS, a system service that runs during computer startup and always runs after that. This service manages activation of COM objects and the running object table and provides helper services to DCOM remoting. It exposes RPC interfaces that can be called remotely. Because some COM servers allow unauthenticated remote component activation

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\Software\policies\Microsoft\windows
NT\DCOM:MachineLaunchRestriction
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\DCOM: Machine Launch Restrictions in Security Descriptor Definition Language
(SDDL) syntax
```

Impact:

Windows operating systems implement default COM ACLs when they are installed. Modifying these ACLs from the default may cause some applications to components that communicate by using DCOM to fail. If you implement a COM server and you override the default security settings, confirm that the application-specific launch permissions ACL assigns activation permission to appropriate users. If it does not, you need to change your application-specific launch permission ACL to provide appropriate users with activation rights so that applications and Windows components that use DCOM do not fail.

1.1.1.2.1.37 Set 'System settings: Optional subsystems' to '' (Scored)

Profile Applicability:

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

Description:

This policy setting determines which subsystems are used to support applications in your environment. Note: 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.

Rationale:

The POSIX subsystem is an Institute of Electrical and Electronic Engineers (IEEE) standard that defines a set of operating system services. The POSIX subsystem is required if the server supports applications that use that subsystem. The POSIX subsystem introduces a security risk that relates to processes that can potentially persist across logons. If a user starts a process and then logs out, there is a potential that the next user who logs on to the computer could access the previous user's process. This potential is dangerous, because anything the second user does with that process will be performed with the privileges of the first user.

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\System\CurrentControlSet\Control\Session
Manager\SubSystems:optional
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to .

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

Impact:

Applications that rely on the POSIX subsystem will no longer operate. For example, Microsoft Services for Unix (SFU) installs an updated version of the POSIX subsystem that is required, so you would need to reconfigure this setting in a Group Policy for any servers that use SFU.

1.1.1.2.1.38 Set 'Devices: Allowed to format and eject removable media' 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 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.

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 object is backed by the following registry location:

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

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `0`.

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

Impact:

Only Administrators will be able to format and eject removable media. If users are in the habit of using removable media for file transfers and storage, they will need to be informed of the change in policy.

1.1.1.2.1.39 Set 'Microsoft network client: Digitally sign communications (always)' 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. If you enable this policy setting, the Microsoft network client computer cannot communicate with a Microsoft network server unless that server agrees to sign SMB

packets. In mixed environments with legacy client computers, set this option to Disabled because these computers will not be able to authenticate or gain access to domain controllers. However, you can use this policy setting in Windows 2000 or later environments. 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.

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 forward them 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 the Windows operating systems. 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 object is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters:Requ
ireSecuritySignature
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `1`.

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

Impact:

The Windows 2000 and later implementations of the SMB file and print sharing protocol support mutual authentication, which protect against session hijacking attacks and support 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 Knowledgebase Article 950876 for more details: http://support.microsoft.com/default.aspx/kb/950876/.

1.1.1.2.1.40 Set 'Interactive logon: Prompt user to change password before expiration' to '14' (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 14 days to sufficiently warn users when their passwords will expire.

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 object is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon:passwordexpirywarning
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `14`.

```
Computer Configuration\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 in 14 or fewer days.

1.1.1.2.1.41 Set 'Domain member: Maximum machine account password age' to '30' (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. If you increase this interval significantly or set it to 0 so that the computers no longer change their passwords, an attacker would have more time to undertake a brute force attack against one of the computer accounts.

Rationale:

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

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, set the following Group Policy setting to `30`.

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

Impact:

None. This is the default configuration.

1.1.1.2.1.42 Set 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' to 'Enabled' (Scored)

Profile Applicability:

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

Description:

The registry value entry SafeDllSearchMode was added to the template file in the HKEY_LOCAL_MACHINE\ SYSTEM\CurrentControlSet\Control\Session Manager\ registry key. The entry appears as MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended) in the SCE. 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.

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 object is backed by the following registry location:

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

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `1`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)
```

Impact:

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.

1.1.1.2.1.43 Configure 'Interactive logon: Display user information when the session is locked' (Not 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 can display in each computer's respective Windows logon screen. If you enable this policy setting, intruders cannot collect account names visually from the screens of desktop or laptop computers in your organization.

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 Terminal 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 for your organization. This group policy object is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System:DontDispl
ayLockedUserId
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Interactive logon: Display user information when the session is locked
```

Impact:

Users will always have to type their user names when they log on to the servers.

1.1.1.2.1.44 Set 'MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)' to '3' (Scored)

Profile Applicability:

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

Description:

The registry value entry TCPMaxDataRetransmissions was added to the template file in the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip \Parameters\ registry key. The entry appears as MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default) in the SCE. 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.

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 object is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters:TcpMaxDataRetran
smissions
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to 3.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is
retransmitted (3 recommended, 5 is default)
```

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.

1.1.1.2.1.45 Set 'Domain member: Digitally sign secure channel data (when possible)' 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. Microsoft recommends to configure the Domain member: Digitally sign secure channel data (when possible) setting to 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. If a computer is configured to always encrypt or sign secure channel data but the domain controller cannot sign or encrypt any portion of the secure channel data, the computer and domain controller cannot establish a secure channel. If the computer is configured to encrypt or sign secure channel data when possible, a secure channel can be established, but the level of encryption and signing is negotiated.

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\System\CurrentControlSet\Services\Netlogon\Parameters:signsecurecha
nnel
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `1`.

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

Impact:

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. 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 the 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. You can enable the other two policy settings, Domain member: Digitally encrypt secure channel data (when possible) and Domain member: Digitally encrypt sign channel data (when possible), on all computers in the domain that support them and clients running versions of Windows earlier than Windows NT 4.0 with SP6a and applications that run on these versions of Windows will not be affected.

1.1.1.2.1.46 Set 'Domain member: Digitally encrypt secure channel data (when possible)' 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. If you enable this policy setting, the domain member will request encryption of all secure channel traffic. If you disable this policy setting, the domain member will be prevented from negotiating secure channel encryption. Microsoft recommends to configure the Domain member: Digitally encrypt secure channel data (when possible) setting to Enabled.

Rationale:

When a computer running Windows NT, Windows 2000, or later versions of Windows 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. If a computer is configured to always encrypt or sign secure channel data but the domain controller cannot sign or encrypt any portion of the secure channel data, the computer and domain controller cannot establish a secure channel. If the computer is configured to encrypt or sign secure channel data when possible, a secure channel can be established, but the level of encryption and signing is negotiated.

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\System\CurrentControlSet\Services\Netlogon\Parameters:sealsecurechannel
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `1`.

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

Impact:

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. 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 the 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:

1.1.1.2.1.47 Configure 'Domain controller: LDAP server signing requirements' (Not Scored)

Profile Applicability:

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

Description:

This policy setting determines whether the Lightweight Directory Access Protocol (LDAP) server requires LDAP clients to negotiate data signing.

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.

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\NTDS\Parameters:ldapserverintegri
ty
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Domain controller: LDAP server signing requirements
```

Impact:

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 NTÂ® 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 article 325465, Windows 2000 domain controllers require SP3 or later when using Windows Server 2003 administration tools, in the Microsoft Knowledge Base (http://go.microsoft.com/fwlink/?LinkId=100900). 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.

1.1.1.2.1.48 Set 'Microsoft network client: Send unencrypted password to third-party SMB servers' to 'Disabled' (Scored)

Profile Applicability:

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

Description:

Disable this policy setting to prevent the SMB redirector from sending 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.

Rationale:

If you enable this policy setting, the computer can transmit passwords in plaintext across the network to other computers that offer SMB services. These other computers may not use any of the SMB security mechanisms that are included with recent versions Windows.

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\System\CurrentControlSet\Services\LanmanWorkstation\Parameters:Enab
lePlainTextPassword
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `0`.

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

Impact:

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.

1.1.1.2.1.49 Set 'Interactive logon: Do not require CTRL+ALT+DEL' 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. If you enable this policy setting, users can log on without this key combination. If you disable this policy setting, 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.

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 object is backed by the following registry location:

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

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `0`.

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

Impact:

Unless they use a smart card to log on, users will have to simultaneously press three keys before the logon dialog box will display.

1.1.1.2.1.50 Configure 'Interactive logon: Message title for users attempting to log on' (Not Scored)

Profile Applicability:

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

Description:

Microsoft recommends that you use this setting, if appropriate to your environment and your organization's business requirements, to help protect end user computers. This policy setting allows text to be specified in the title bar of the window that users see when they log on to the system.

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 for your organization. This group policy object is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System:LegalNoti
ceCaption
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

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

Impact:

Users will see a message in a dialog box before they can log on to the server console. Note that Windows XP and later versions of Windows 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. If you inadvertently create a logon message policy on a Windows Vista-based or Windows XP Professional-based computer and you discover that it does not display properly on Windows 2000-based computers, do the following: Change the setting to Not Defined, and then change the setting to the desired value by using a Windows 2000-based computer. Important: If you do not reconfigure this setting to Not Defined before reconfiguring the setting using a Windows 2000-based computer, the changes will not take effect properly.

1.1.1.2.1.51 Configure 'Interactive logon: Message text for users attempting to log on' (Not Scored)

Profile Applicability:

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

Description:

Microsoft recommends that you use this setting, if appropriate to your environment and your organization's business requirements, to help protect end user computers. This policy setting specifies a text message that displays to users when they log on.

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 for your organization. This group policy object is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System:LegalNoti
ceText
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

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

Impact:

Users will see a message in a dialog box before they can log on to the server console. Note that Windows XP and later versions of Windows 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. If you inadvertently create a logon message policy on a Windows Vista-based or Windows XP Professional-based computer and you discover that it does not display properly on Windows 2000-based computers, do the following: Change the setting to Not Defined, and then change the setting to the desired value by using a Windows 2000-based computer. Important: If you do not reconfigure this setting to Not Defined before reconfiguring the setting using a Windows 2000-based computer, the changes will not take effect properly.

1.1.1.2.1.52 Set 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)' to '0' (Scored)

Profile Applicability:

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

Description:

The registry value entry ScreenSaverGracePeriod was added to the template file in the HKEY_LOCAL_MACHINE\SYSTEM\Software\Microsoft\ Windows NT\CurrentVersion\Winlogon\ registry key. The entry appears as MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended) in the SCE. 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. This setting is configured to 0 seconds for both of the environments that are discussed in this guide.

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 object is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon:ScreenSaverGracePeriod
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `0`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver
grace period expires (0 recommended)
```

Impact:

Users will have to enter their passwords to resume their console sessions as soon as the screen saver activates.

1.1.1.2.1.53 Set 'Microsoft network client: Digitally sign communications (if server agrees)' 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. The implementation of digital signing in Windows based networks helps to prevent sessions from being hijacked. If you enable this policy setting, the Microsoft network client will use signing only if the server with which it communicates accepts digitally signed communication. Microsoft recommends to enable The Microsoft network client: Digitally sign communications (if server agrees) setting. 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.

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 them 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. 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 object is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters:Enab
leSecuritySignature
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `1`.

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

Impact:

The Windows 2000 and later implementations of the SMB file and print sharing protocol support mutual authentication, which protect against session hijacking attacks and support 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 Knowledgebase Article 950876 for more details: http://support.microsoft.com/default.aspx/kb/950876/.

1.1.1.2.1.54 Set 'Domain member: Digitally encrypt or sign secure channel data (always)' 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. If a system is set to always encrypt or sign secure channel data, it cannot establish a secure channel with a domain controller that is not capable of signing or encrypting all secure channel traffic, because all secure channel data must be signed and encrypted. Microsoft recommends to configure the Domain member: Digitally encrypt or sign secure channel data (always) setting to 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. If a computer is configured to always encrypt or sign secure channel data but the domain controller cannot sign or encrypt any portion of the secure channel data, the computer and domain controller cannot establish a secure channel. If the computer is configured to encrypt or sign secure channel data when possible, a secure channel can be established, but the level of encryption and signing is negotiated.

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\System\CurrentControlSet\Services\Netlogon\Parameters:requiresignor
seal
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `1`.

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

Impact:

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. 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 the 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. You can enable the other two policy settings, Domain member: Digitally encrypt secure channel data (when possible) and Domain member: Digitally encrypt sign channel data (when possible), on all computers in the domain that support them and clients running versions of Windows earlier than Windows NT 4.0 with SP6a and applications that run on these versions of Windows will not be affected.

1.1.1.2.1.55 Set 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)' 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. The setting helps secure objects that can be located and shared among processes and its default configuration strengthens the DACL, because it allows users who are not administrators to read shared objects but does not allow them to modify any that they did not create.

Rationale:

This setting determines the strength of the default DACL for objects. Windows Server 2003 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. If you enable this setting, the default DACL is strengthened because non-administrator users are allowed to read shared objects but not modify shared objects that they did not create.

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\System\CurrentControlSet\Control\Session Manager:ProtectionMode
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `1`.

```
Computer Configuration\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 configuration.

1.1.1.2.1.56 Set 'Network security: Do not store LAN Manager hash value on next password change' 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. Note Older operating systems and some third-party applications may fail when this policy setting is enabled. Also you will need to change the password on all accounts after you enable this setting.

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 object is backed by the following registry location:

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

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `1`.

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

Impact:

Earlier operating systems such as Windows 95, Windows 98, and Windows ME as well as some third-party applications will fail.

1.1.1.2.1.57 Set 'Network access: Remotely accessible registry paths and sub-paths' to 'System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Services\Eventlog Software\Microsoft\OLAP Server Software\Microsoft\Windows NT\CurrentVersion\Print Sof (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 when an application or process references the WinReg key to determine access permissions. 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, and Windows Server 2003 does not exist in Windows XP. Note: 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.

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 object is backed by the following registry location:

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

Remediation:

To implement the recommended configuration state, set the following Group Policy setting 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\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Remotely accessible registry paths and sub-paths
```

Impact:

Remote management tools such as the Microsoft Baseline Security Analyzer and Microsoft Systems Management Server require remote access to the registry to properly monitor and manage those computers. If you remove the default registry paths from the list of accessible ones, such remote management tools could fail. Note: If you want to allow remote access, you must also enable the Remote Registry service.

1.1.1.2.1.58 Configure 'System cryptography: Force strong key protection for user keys stored on the computer' (Not Scored)

Profile Applicability:

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

Description:

This policy setting determines whether users' private keys (such as their S-MIME keys) require a password to be used. If you configure this policy setting so that users must provide a password distinct from their domain password every time that they use a key, then it will be more difficult for an attacker to access locally stored keys, even an attacker who discovers logon passwords.

Rationale:

If a users account is compromised or their computer is inadvertently left unsecured the malicious user can use the keys stored for the user to access protected resources. You can configure this policy setting so that users must provide a password that is distinct from their domain password every time they use a key. This configuration makes it more difficult for an attacker to access locally stored user keys, even if the attacker takes control of the user's computer and determines their logon password.

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\Software\Policies\Microsoft\Cryptography:ForceKeyProtection
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\System cryptography: Force strong key protection for user keys stored on the
computer
```

Impact:

Users will have to enter their password every time they access a key that is stored on their computer. For example, if users use an S-MIME certificate to digitally sign their e-mail they will be forced to enter the password for that certificate every time they send a signed e-mail message. For some organizations the overhead that is involved using this configuration may be too high. For end user computers that are used to access sensitive data this setting could be set to "User is prompted when the key is first used," but Microsoft does not recommend enforcing this setting on servers due to the significant impact on manageability. For example, if this setting is configured to "User is prompted when the key is first used" you may not be able to configure Remote Desktop Services to use SSL certificates. More information is available in the Windows PKI blog: http://blogs.technet.com/b/pki/archive/2009/06/17/what-is-a-strong-key-protection-in-windows.aspx.

1.1.1.2.1.59 Set 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' to 'Highest protection, source routing is completely disabled' (Scored)

Profile Applicability:

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

Description:

The registry value entry DisableIPSourceRouting was added to the template file in the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\ registry key. The entry appears as MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing) in the SCE. 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.

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 object is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters:DisableIPSourceR
outing
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `2`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\MSS: (DisableIPSourceRouting) IP source routing protection level (protects
against packet spoofing)
```

Impact:

If you configure this value to 2, all incoming source routed packets will be dropped.

1.1.1.2.1.60 Set 'MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)' to 'Disabled' (Scored)

Profile Applicability:

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

Description:

The registry value entry PerformRouterDiscovery was added to the template file in the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\ registry key. The entry appears as MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS) in the SCE. 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.

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 object is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters:PerformRouterDis
covery
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `0`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default
Gateway addresses (could lead to DoS)
```

Impact:

If you disable this entry, Windows cannot automatically detect and configure default gateway addresses on the computer.

1.1.1.2.1.61 Set 'MSS: (TcpMaxConnectResponseRetransmissions) SYN-ACK retransmissions when a connection request is not acknowledged' to '3 & 6 seconds, half-open connections dropped after 21 seconds' (Scored)

Profile Applicability:

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

Description:

This entry appears as MSS: (TcpMaxConnectResponseRetransmissions) SYN-ACK retransmissions when a connection request is not acknowledged in the SCE. This entry determines the number of times that TCP retransmits a SYN before it aborts the attempt. The retransmission time-out is doubled with each successive retransmission in a given connect attempt. The initial time-out value is three seconds. Not applicable to Windows Vista or Windows Server 2008.

Rationale:

In a SYN flood attack, the attacker sends a continuous stream of SYN packets to a server. The server leaves the half-open connections open until it is overwhelmed and no longer is able to respond to legitimate requests.

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\System\CurrentControlSet\Services\Tcpip\Parameters:TcpMaxConnectResponseRetransmissions
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `2`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\MSS: (TcpMaxConnectResponseRetransmissions) SYN-ACK retransmissions when a connection request is not acknowledged
```

Impact:

If you configure this value to greater than or equal to 2, the stack will employ SYN-ATTACK protection internally. If you configure this entry to less than 2, the stack cannot read the registry values at all for SYN-ATTACK protection. This entry shortens the default amount of time that is needed to clean up a half-open TCP connection. A site that is under heavy attack might set the value as low as 1. A value of 0 is also valid. However, if this parameter is set to 0, SYN-ACKs will not be retransmitted at all and will time out in 3 seconds. If the value is this low, legitimate connection attempts from distant clients may fail.

1.1.1.2.1.62 Set 'Microsoft network server: Disconnect clients when logon hours expire' to 'Enabled' (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. It affects the SMB component. If you enable this policy setting, client sessions with the SMB service will be forcibly disconnected when the client's logon hours expire. If you disable this policy setting, established client sessions will be maintained after the client's logon hours expire. If you enable this policy setting you should also enable Network security: Force logoff when logon hours expire. If your organization configures logon hours for users, it makes sense to enable this policy setting.

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 object is backed by the following registry location:

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

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `1`.

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

Impact:

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.

1.1.1.2.1.63 Set 'Network access: Let Everyone permissions apply to anonymous users' 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. If you enable this policy setting, anonymous Windows users are allowed to perform certain activities, such as enumerate the names of domain accounts and network shares. An unauthorized user could anonymously list account names and shared resources and use the information to guess passwords or perform social engineering attacks.

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 denial of service (DoS) attacks.

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\System\CurrentControlSet\Control\Lsa:EveryoneIncludesAnonymous
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `0`.

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

Impact:

None. This is the default configuration.

1.1.1.2.1.64 Set 'Microsoft network server: Digitally sign communications (always)' to 'Enabled' (Scored)

Profile Applicability:

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

Description:

This policy setting determines if the server side SMB service is required to perform SMB packet signing. Enable this policy setting in a mixed environment to prevent downstream clients from using the workstation as a network server.

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. 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 object is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters:requirese
curitysignature
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `1`.

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

Impact:

The Windows 2000 and later implementations of the SMB file and print sharing protocol support mutual authentication, which protect against session hijacking attacks and support 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 Knowledgebase Article 950876 for more details: http://support.microsoft.com/default.aspx/kb/950876/.

1.1.1.2.1.65 Set 'Network security: LDAP client signing requirements' to 'Negotiate signing' (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, as follows: . None. The LDAP BIND request is issued with the caller-specified options. . 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. . Require signature. This level is the same as Negotiate signing. However, if the LDAP server's

intermediate saslBindInProgress response does not indicate that LDAP traffic signing is required, the caller is told that the LDAP BIND command request failed. Note: This policy setting does not have any impact on ldap_simple_bind or 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 possible values for the Network security: LDAP client signing requirements setting are: . None . Negotiate signing . Require signature . Not Defined

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 object is backed by the following registry location:

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

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `1`.

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

Impact:

If you configure the server to require LDAP signatures 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.

1.1.1.2.1.66 Set 'Devices: Allow undock without having to log on' to 'Disabled' (Scored)

Profile Applicability:

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

Description:

This policy setting determines whether a portable computer can be undocked if the user does not log on to the system. Enable this policy setting to eliminate a Logon requirement and allow use of an external hardware eject button to undock the computer. If you disable this policy setting, a user must log on and have been assigned the Remove computer from docking station user right to undock the computer.

Rationale:

If this policy setting is enabled, anyone with physical access to portable computers in docking stations could remove them and possibly tamper with them. However, the value of implementing this countermeasure is reduced by the following factors: . If attackers can restart the computer, they could remove it from the docking station after the BIOS starts but before the operating system starts. . This setting does not affect servers, because they typically are not installed in docking stations. . An attacker could steal the computer and the docking station together.

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\Microsoft\Windows\CurrentVersion\Policies\System:undockwit
houtlogon
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `0`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Devices: Allow undock without having to log on
```

Impact:

Users who have docked their computers will have to log on to the local console before they can undock their computers. For computers that do not have docking stations, this policy setting will have no impact.

1.1.1.2.1.67 Set 'Audit: Audit the access of global system objects' to 'Disabled' (Scored)

Profile Applicability:

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

Description:

This policy setting creates a default system access control list (SACL) for system objects such as mutexes (mutual exclusive), events, semaphores, and MS-DOS devices, and causes access to these system objects to be audited. If the Audit: Audit the access of global system objects setting is enabled, a very large number of security events could quickly fill the Security event log.

Rationale:

A globally visible named object, if incorrectly secured, could be acted upon by malicious software that knows the name of the object. For instance, if a synchronization object such as a mutex had a poorly chosen discretionary access control list (DACL), then malicious software could access that mutex by name and cause the program that created it to malfunction. However, the risk of such an occurrence is very low.

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\System\CurrentControlSet\Control\Lsa:AuditBaseObjects
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `0`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Audit: Audit the access of global system objects
```

Impact:

If you enable the Audit: Audit the access of global system objects setting, a large number of security events could be generated, especially on busy domain controllers and application servers. Such an occurrence could cause servers to respond slowly and force the Security log to record numerous events of little significance. This policy setting can only be enabled or disabled, and there is no way to choose which events are recorded. Even organizations that have the resources to analyze events that are generated by this policy setting would not likely have the source code or a description of what each named object is used for. Therefore, it is unlikely that many organizations could benefit by enabling this policy setting.

1.1.1.2.1.68 Set 'MSS: (AutoReboot) Allow Windows to automatically restart after a system crash (recommended except for highly secure environments)' to 'Enabled' (Scored)

Profile Applicability:

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

Description:

This entry appears as MSS: (AutoReboot) Allow Windows to automatically restart after a system crash (recommended except for highly secure environments) in the SCE. This entry, when enabled, permits a server to automatically reboot after a fatal crash. It is enabled by default, which is undesirable on highly secure servers. You can add this registry value to the template file in the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\CrashControl\ subkey.

Rationale:

There is some concern that a computer could get stuck in an endless loop of failures and reboots. However, the alternative to this entry may not be much more appealing the computer will simply stop running.

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\SYSTEM\CurrentControlSet\Control\CrashControl:AutoReboot
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `1`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\MSS: (AutoReboot) Allow Windows to automatically restart after a system crash
(recommended except for highly secure environments)
```

Impact:

The computer will no longer reboot automatically after a failure.

1.1.1.2.1.69 Set 'Interactive logon: Require smart card' to 'Disabled' (Scored)

Profile Applicability:

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

Description:

Microsoft recommends that you use this setting, if appropriate to your environment and your organization's business requirements, to help protect end user computers. This policy setting requires users to log on to a computer with a smart card. Note: This setting applies to Windows 2000 computers, but it is not available through the Security Configuration Manager tools on these computers.

Rationale:

It can be difficult to make users choose strong passwords, and even strong passwords are vulnerable to brute-force attacks if an attacker has sufficient time and computing resources.

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\Microsoft\Windows\CurrentVersion\Policies\System:scforceop
tion
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `0`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Interactive logon: Require smart card
```

Impact:

All users of a computer with this setting enabled will have to use smart cards to log onto the local computer, which means that the organization will need a reliable public key infrastructure (PKI) as well as smart cards and smart card readers for these users. These requirements are significant challenges, because expertise and resources are required to plan for and deploy these technologies. However, Windows Server 2003 and later versions of Windows Server includes Certificate Services, a highly advanced service for implementing and managing certificates. When Certificate Services is combined with client computers that run Windows, features such as automatic user and computer enrollment and renewal become available. For more information about deploying Smart Cards with Windows Vista see the paper "Windows Vista Smart Card Infrastructure" available for download at the Microsoft Web site (http://www.microsoft.com/downloads/details.aspx?FamilyID=ac201438-3317-44d3-9638-07625fe397b9&displaylang=en).

1.1.1.2.1.70 Configure 'Devices: Restrict floppy access to locally logged-on user only' (Not Scored)

Profile Applicability:

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

Description:

This policy setting determines whether removable floppy media are accessible to both local and remote users simultaneously. If you enable this policy setting, only the interactively logged-on user is allowed to access removable floppy media. If this policy setting is enabled and no one is logged on interactively, the floppy media is accessible over the network.

Rationale:

A remote user could potentially access a mounted floppy that contains sensitive information. This risk is small because floppy disk drives are not automatically shared; administrators must deliberately choose to share the drive. However, administrators may wish to deny network users the ability to view data or run applications from removable media on the server.

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\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon:AllocateFloppies
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Devices: Restrict floppy access to locally logged-on user only
```

Impact:

Users who connect to the server over the network will not be able to use any floppy disk drives that are installed on the server whenever anyone is logged on to the local console of the server. System tools that require access to floppy disk drives will fail. For example, the Volume Shadow Copy service attempts to access all CD-ROM and floppy disk drives present on the computer when it initializes, and if the service cannot access one of these drives it will fail. This condition will cause the Windows Backup tool to fail if volume shadow copies were specified for the backup job. Any non-Microsoft backup products that use volume shadow copies will also fail.

1.1.1.2.1.71 Set 'Network access: Allow anonymous SID/Name translation' 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. Disable this policy setting to prevent unauthenticated users from obtaining user names that are associated with their respective SIDs.

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 implement the recommended configuration state, set the following Group Policy setting to `False`.

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

Impact:

Disabled is the default configuration for this policy setting on member computers; therefore it will have no impact on them. If you disable this policy setting on domain controllers, legacy computers may be unable to communicate with other computers in the domain. For example, the following computers may not work: . Windows NT 4.0based Remote Access Service servers. . Microsoft SQL Servers that run on Windows NT 3.xbased or Windows NT 4.0based computers. . Remote Access Service or Microsoft SQL servers that run on Windows 2000based computers and are located in Windows NT 3.x domains or Windows NT 4.0 domains.

1.1.1.2.1.72 Set 'Domain member: Require strong (Windows 2000 or later) session key' 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 later. If communication to non-Windows 2000based domains is required, it is recommended that you disable this policy setting.

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 object is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters:requirestrong
key
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `1`.

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

Impact:

Computers that have this policy setting enabled 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, computers that do not support this policy setting will not be able to join domains in which the domain controllers have this policy setting enabled.

1.1.1.2.1.73 Set 'Network access: Remotely accessible registry paths' to 'System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications Software\Microsoft\Windows NT\CurrentVersion' (Scored)

Profile Applicability:

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

Description:

This policy setting determines which registry paths will be accessible after referencing the WinReg key to determine access permissions to the paths. 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 subpaths in Windows Server 2003, Windows Vista, and Windows Server 2008. Note: 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.

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 object is backed by the following registry location:

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

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications Software\Microsoft\Windows NT\CurrentVersion`.

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

Impact:

Remote management tools such as the Microsoft Baseline Security Analyzer and Microsoft Systems Management Server require remote access to the registry to properly monitor and manage those computers. If you remove the default registry paths from the list of accessible ones, such remote management tools could fail. Note: If you want to allow remote access, you must also enable the Remote Registry service.

1.1.1.2.1.74 Set 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' to '0' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

Rationale:

The number that is assigned to this policy setting indicates the number of users whose logon information the servers will cache locally. If the number is set to 10, then the server caches logon information for 10 users. When an eleventh user logs on to the computer, the server overwrites the oldest cached logon session. Users who access the server console will have their logon credentials cached on that server. 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 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 object is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon:cachedlogonscount
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `0`.

```
Computer Configuration\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.

1.1.1.2.1.75 Configure 'Network access: Named Pipes that can be accessed anonymously' (Not Scored)

Profile Applicability:

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

Description:

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

Rationale:

You can restrict access over named pipes such as COMNAP and LOCATOR to help prevent unauthorized access to the network. The list of some of the default named pipes and their purpose is provided in the following list: Browser - Named pipe for the Computer Browser service. COMNAP - SNABase named pipe. Systems Network Architecture (SNA) is a collection of network protocols that were originally developed for IBM mainframe computers. COMNODE - SNA Server named pipe. EPMAPPER - End Point Mapper named pipe. LOCATOR - Remote Procedure Call Locator service named pipe. Lsarpc - Named pipe for the Local Security Authority Remote Procedure Call service. Netlogon - Named pipe for then NetLogon service. Samr - Named pipe for the Security Accounts Manager service. SPOOLSS - Named pipe for the Print Spooler service. SQL\QUERY - Default named pipe for SQL Server. Srvsvc - Named pipe for the Server service. TrkSvr - Distributed Link Tracking

Server named pipe. TrkWks - Distributed Link Tracking Client named pipe. Wkssvc - Named pipe for the Workstation service.

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\LanManServer\Parameters:NullSessionPipes
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

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

Impact:

This configuration will disable null session access over named pipes, and applications that rely on this feature or on unauthenticated access to named pipes will no longer function. For example, with Microsoft Commercial Internet System 1.0, the Internet Mail Service runs under the Inetinfo process. Inetinfo starts in the context of the System account. When Internet Mail Service needs to query the Microsoft SQL Server database, it uses the System account, which uses null credentials to access a SQL pipe on the computer that runs SQL Server. To avoid this problem, refer to the Microsoft Knowledge Base article How to access network files from IIS applications, which is located at http://support.microsoft.com/default.aspx?scid=207671.

1.1.1.2.1.76 Set 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- 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 workstations in

your environment. The Network access: Do not allow anonymous enumeration of SAM accounts and shares setting is configured to Enabled for the two environments that are discussed in this guide.

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.

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\System\CurrentControlSet\Control\Lsa:RestrictAnonymous
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `1`.

```
Computer Configuration\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 grant access to users of another domain across a one-way trust because administrators in the trusting domain will be unable to enumerate lists of accounts in the other domain. 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.

1.1.1.2.1.77 Set 'Recovery console: Allow automatic administrative logon' to 'Disabled' (Scored)

Profile Applicability:

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

Description:

The recovery console is a command-line environment that is used to recover from system problems. If you enable this policy setting, the administrator account is automatically logged on to the recovery console when it is invoked during startup.

Rationale:

The Recovery Console can be very useful when you need to troubleshoot and repair computers that do not start. However, it is dangerous to allow automatic logon to the console. Anyone could walk up to the server, disconnect the power to shut it down, restart it, select Recover Console from the Restart menu, and then assume full control of the server.

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\Microsoft\Windows
NT\CurrentVersion\Setup\RecoveryConsole:securitylevel
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `0`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Recovery console: Allow automatic administrative logon
```

Impact:

Users will have to enter a user name and password to access the Recovery Console.

1.1.1.2.1.78 Set 'Audit: Shut down system immediately if unable to log security audits' 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. Therefore, this policy setting is configured to Not Defined for both of the environments that are discussed in this chapter.

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 object is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa:crashonauditfail
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `0`.

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

Impact:

If you enable this policy setting, 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.

1.1.1.2.1.79 Set 'Microsoft network server: Digitally sign communications (if client agrees)' to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller

- Level 1 - Member Server

Description:

This policy setting determines if the server side SMB service is able to sign SMB packets if it is requested to do so by a client that attempts to establish a connection. 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.

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 them 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. 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 object is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters:enablesec
uritysignature
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `1`.

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

Impact:

The Windows 2000 and later implementations of the SMB file and print sharing protocol support mutual authentication, which protect against session hijacking attacks and support 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 Knowledgebase Article 950876 for more details: http://support.microsoft.com/default.aspx/kb/950876/.

1.1.1.2.1.80 Set 'Network access: Sharing and security model for local accounts' 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.

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 object is backed by the following registry location:

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

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `0`.

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

Impact:

None. This is the default configuration.

1.1.1.2.1.81 Set 'Network access: Do not allow anonymous enumeration of SAM accounts' to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- 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 cannot enumerate domain account user names on the workstations in your environment. This policy setting also allows additional restrictions on anonymous connections.

Rationale:

An unauthorized user could anonymously list account names and use the information to perform social engineering attacks or attempt to guess passwords. (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 object is backed by the following registry location:

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

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `1`.

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

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.

1.1.1.2.1.82 Set 'Interactive logon: Require Domain Controller authentication to unlock workstation' to 'Enabled' (Scored)

Profile Applicability:

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

Description:

Logon information is required to unlock a locked computer. For domain accounts, the Interactive logon: Require Domain Controller authentication to unlock workstation setting determines whether it is necessary to contact a domain controller to unlock a computer. If you enable this setting, a domain controller must authenticate the domain account that is being used to unlock the computer. If you disable this setting, logon information confirmation with a domain controller is not required for a user to unlock the computer. However, if you configure the Interactive logon: Number of previous logons to cache (in case domain controller is not available) setting to a value that is greater than zero, then the user's cached credentials will be used to unlock the computer. Note: This setting applies to Windows 2000 computers, but it is not available through the Security Configuration Manager tools on these computers.

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 object is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon:ForceUnlockLogon
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `1`.

```
Computer Configuration\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 the user is able to re-authenticate to the domain controller. If no domain controller is available, then users cannot unlock their workstations. If you configure the Interactive logon: Number of previous logons to cache (in case domain controller is not available) setting to 0, users whose domain controllers are unavailable (such as mobile or remote users) will not be able to log on.

1.1.1.2.1.83 Set 'Network access: Do not allow storage of credentials or .NET Passports for network authentication' to 'Enabled' (Scored)

Profile Applicability:

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

Description:

This policy setting determines whether the Stored User Names and Passwords feature may save passwords or credentials for later use when it gains domain authentication. If you enable this policy setting, the Stored User Names and Passwords feature of Windows does not store passwords and credentials.

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 object is backed by the following registry location:

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

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `1`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Network access: Do not allow storage of credentials or .NET Passports for
network authentication
```

Impact:

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.

1.1.1.2.1.84 Set 'MSS: (EnableDeadGWDetect) Allow automatic detection of dead network gateways (could lead to DoS)' to 'Disabled' (Scored)

Profile Applicability:

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

Description:

This entry appears as MSS: (EnableDeadGWDetect) Allow automatic detection of dead network gateways (could lead to DoS) in the SCE. When dead gateway detection is enabled, the IP may change to a backup gateway if a number of connections experience difficulty. Not applicable to Windows Vista or Windows Server 2008.

Rationale:

An attacker could force the server to switch gateways, potentially to an unintended one. This would be very difficult to do, so the value of this entry is small.

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\System\CurrentControlSet\Services\Tcpip\Parameters:EnableDeadGWDete
ct
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `0`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\MSS: (EnableDeadGWDetect) Allow automatic detection of dead network gateways
(could lead to DoS)
```

Impact:

If you configure this value to 0, Windows cannot detect dead gateways and automatically switch to alternates.

1.1.1.2.1.85 Set 'System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing' to 'Disabled' (Scored)

Profile Applicability:

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

Description:

This policy setting determines whether the Transport Layer Security/Secure Sockets Layer (TLS/SSL) Security Provider supports only the TLS_RSA_WITH_3DES_EDE_CBC_SHA cipher suite. Although this policy setting increases security, most public Web sites that are secured with TLS or SSL do not support these algorithms. Client computers that have this

policy setting enabled will also be unable to connect to Terminal Services on servers that are not configured to use the FIPS compliant algorithms. Note If you enable this policy setting, computer performance will be slower because the 3DES process is performed on each block of data in the file three times. This policy setting should only be enabled if your organization is required to be FIPS compliant. Important: This setting is recorded in different registry locations depending upon the version of Windows being used. For Windows XP and Windows Server 2003 it is stored at HKLM\System\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy, with Windows Vista and later versions of Windows it is stored at HKLM\System\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy\Enabled. This means that you must use Windows XP or Windows Server 2003 to edit group policies and security templates which will be applied to computers running Windows XP or Windows Server 2003. However, when editing group policies or security templates which will be applied to computers running Windows Vista or Windows Server 2008 you must use Windows Vista or Windows Server 2008.

Rationale:

You can enable this policy setting to ensure that the computer will use the most powerful algorithms that are available for digital encryption, hashing and signing. Use of these algorithms will minimize the risk of compromise of digitally encrypted or signed data by an unauthorized user.

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\System\CurrentControlSet\Control\Lsa:FIPSAlgorithmPolicy
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `0`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\System cryptography: Use FIPS compliant algorithms for encryption, hashing,
and signing
```

Impact:

Client computers that have this policy setting enabled will be unable to communicate by means of digitally encrypted or signed protocols with servers that do not support these algorithms. Network clients that do not support these algorithms will not be able to use

servers that require them for network communications. For example, many Apache-based Web servers are not configured to support TLS. If you enable this setting, you also need to configure Internet Explorer to use TLS. This policy setting also affects the encryption level that is used for the Remote Desktop Protocol (RDP). The Remote Desktop Connection tool uses the RDP protocol to communicate with servers that run Terminal Services and client computers that are configured for remote control; RDP connections will fail if both computers are not configured to use the same encryption algorithms. To enable Internet Explore to use TLS 1. On the Internet Explorer Tools menu, click Internet Options. 2. Click the Advanced tab. 3. Select the Use TLS 1.0 check box. It is also possible to configure this policy setting through Group Policy or by using the Internet Explorer Administrators Kit. Client computers running Windows XP, Windows XP SP1 and Windows XP SP2 that try to connect to a Terminal Services server that has this setting enabled will be unable to communicate with the server until an updated version of the Terminal Services client is installed. This issue could aslo affect Remote Assistance and Remote Desktop connections. For more information about the issue and how to resolve it see "Remote Assistance connection to Windows Server 2003 with FIPS encryption does not work" at http://support.microsoft.com/default.aspx?scid=kb;en-us;811770.

1.1.1.2.1.86 Set 'Audit: Audit the use of Backup and Restore privilege' to 'Disabled' (Scored)

Profile Applicability:

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

Description:

This policy setting determines whether to audit the use of all user privileges, including Backup and Restore, when the Audit privilege use setting is in effect. If you enable both policies, an audit event will be generated for every file that is backed up or restored. If the Audit: Audit the use of Backup and Restore privilege setting is enabled, a very large number of security events could quickly fill the Security event log.

Rationale:

When back up and restore is used it creates a copy of the file system that is identical to the target of the backup. Making regular backups and restore volumes is an important part of a your incident response plan, but a malicious user could use a legitimate backup copy to get access to information or spoof a legitimate network resource to compromise your enterprise.

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\System\CurrentControlSet\Control\Lsa:fullprivilegeauditing
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `00`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Audit: Audit the use of Backup and Restore privilege
```

Impact:

If you enable this policy setting, a large number of security events could be generated, which could cause servers to respond slowly and force the Security event log to record numerous events of little significance. If you increase the Security log size to reduce the chances of a system shutdown, an excessively large log file may affect system performance.

1.1.1.2.1.87 Set 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' to 'Disabled' (Scored)

Profile Applicability:

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

Description:

The registry value entry EnableICMPRedirect was added to the template file in the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\ registry key. The entry appears as MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes in the SCE. Internet Control Message Protocol (ICMP) redirects cause the stack to plumb host routes. These routes override the Open Shortest Path First (OSPF)generated routes. It is recommended to configure this setting to Not Defined for enterprise environments and to Disabled for high security environments.

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.

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\System\CurrentControlSet\Services\Tcpip\Parameters:EnableICMPRedire
ct
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `0`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated
routes
```

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.

1.1.1.2.1.88 Set 'MSS: (NoDefaultExempt) Configure IPSec exemptions for various types of network traffic.' to 'Only ISAKMP is exempt (recommended for Windows Server 2003)' (Scored)

Profile Applicability:

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

Description:

The registry value entry NoDefaultExempt was added to the template file in the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\IPSEC\ registry key. The entry appears as MSS: (NoDefaultExempt) Configure IPSec exemptions for various types of network traffic in the SCE. The default exemptions to IPsec policy filters are documented in the online help for the specific operating system. These filters make it possible for Internet Key Exchange (IKE) and the Kerberos authentication protocol to function. The filters also make it possible for the network Quality of Service (QoS) to be signaled (RSVP) when the data traffic is secured by IPsec, and for traffic that IPsec might not secure such as multicast

and broadcast traffic. IPsec is increasingly used for basic host-firewall packet filtering, particularly in Internet-exposed scenarios, and the affect of these default exemptions has not been fully understood. Therefore, some IPsec administrators may create IPsec policies that they think are secure, but are not actually secure against inbound attacks that use the default exemptions. For additional information, see the Knowledge Base article 811832, IPSec Default Exemptions Can Be Used to Bypass IPsec Protection in Some Scenarios.

Rationale:

As IPsec is increasingly used for basic host-firewall packet filtering, particularly in Internet-exposed scenarios, the affect of these default exemptions has not been fully understood. Some IPsec administrators may create IPsec policies that they think are secure, but are not actually secure against inbound attacks that use the default exemptions. Attackers could forge network traffic that appears to consist of legitimate IKE, RSVP, or Kerberos protocol packets but direct them to other network services on the host.

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\System\CurrentControlSet\Services\IPSEC:NoDefaultExempt
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to 3.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\MSS: (NoDefaultExempt) Configure IPSec exemptions for various types of network
traffic.
```

Impact:

After you enable this entry, security policies that already exist may have to be changed to work correctly. For details, refer to the Microsoft Knowledge Base article "IPSec Default Exemptions Can Be Used to Bypass IPsec Protection in Some Scenarios" at http://support.microsoft.com/default.aspx?kbid=811832.

1.1.1.2.2 Audit Policy

1.1.1.2.2.1 Set 'Audit directory service access' to 'Failure' (Scored)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This policy setting determines whether to audit user access to an Active Directory object that has its own specified system access control list (SACL). If you define the Audit directory service access setting, you can specify whether to audit successes, failures, or not audit the event type at all. Success audits generate an audit entry when a user successfully accesses an Active Directory object that has a specified SACL. Failure audits generate an audit entry when a user unsuccessfully attempts to access an Active Directory object that has a specified SACL. If you enable the Audit directory service access setting in the DCBP and configure SACLs on directory objects, a large volume of entries can be generated in the Security logs on domain controllers. You should only enable this setting if you actually intend to use the information that is created. The following includes important security events that the Audit directory service access setting records in the Security log: Event ID Event description ID Description 566 A generic object operation took place.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

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, set the following Group Policy setting to `Failure`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit
Policy\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.

1.1.1.2.2.2 Configure 'Audit directory service access' (Not Scored)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy setting determines whether to audit user access to an Active Directory object that has its own specified system access control list (SACL). If you define the Audit directory service access setting, you can specify whether to audit successes, failures, or not audit the event type at all. Success audits generate an audit entry when a user successfully accesses an Active Directory object that has a specified SACL. Failure audits generate an audit entry when a user unsuccessfully attempts to access an Active Directory object that has a specified SACL. If you enable the Audit directory service access setting in the DCBP and configure SACLs on directory objects, a large volume of entries can be generated in the Security logs on domain controllers. You should only enable this setting if you actually intend to use the information that is created. The following includes important security events that the Audit directory service access setting records in the Security log: Event ID Event description ID Description 566 A generic object operation took place.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer

performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

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

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit
Policy\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.

1.1.1.2.2.3 Set 'Audit account logon events' to 'Success, Failure' (Scored)

Profile Applicability:

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

Description:

This policy setting determines whether to audit each instance of a user who logs on to or off from another computer that validates the account. Authentication of a domain user account on a domain controller generates an account logon event that is logged in the domain controller's Security log. Authentication of a local user on a local computer

generates a logon event that is logged in the local Security log. No account logoff events are logged. The following table includes the important security events that this policy setting logs in the Security log. These event IDs can be useful when you want to create custom alerts to monitor any software suite, such as Microsoft Operations Manager (MOM). Table 4.3 Account Logon Events Event ID Event description 672 An authentication service (AS) ticket was successfully issued and validated. In Windows Server 2003 with SP1, the type of this event will be Success Audit for successful requests or Failure Audit for failed requests. 673 A ticket granting service (TGS) ticket was granted. A TGS is a ticket that is issued by the Kerberos version 5 TGS that allows a user to authenticate to a specific service in the domain. Windows Server 2003 with SP1 will log successes and failures for this event type. 674 A security principal renewed an AS ticket or a TGS ticket. 675 Pre-authentication failed. This event is generated on a Key Distribution Center (KDC) when a user enters an incorrect password. 676 Authentication ticket request failed. This event is not generated by Windows Server 2003 with SP1. Other Windows versions use this event to indicate an authentication failure that was not due to incorrect credentials. 677 A TGS ticket was not granted. This event is not generated by Windows Server 2003 with SP1, which uses a failure audit event with ID 672 for this case. 678 An account was successfully mapped to a domain account. 681 Logon failure. A domain account logon was attempted. This event is only generated by domain controllers. 682 A user has reconnected to a disconnected Terminal Server session. 683 A user disconnected a Terminal Server session but did not log off.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

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, set the following Group Policy setting to `Success, Failure`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit
Policy\Audit account logon 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.

1.1.1.2.2.4 Set 'Audit logon events' to 'Success, Failure' (Scored)

Profile Applicability:

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

Description:

The prescribed GPOs from Microsoft include settings that configure the audit categories present in previous versions of Windows. If you use the script and the GPOs included with this security guidance, these settings will not apply to computers running Windows Vista. The GPOs intended for use in enterprise environments have been designed to work with Windows Searches computers. Settings for audit categories are included in these GPOs so that computers running Windows XP in your environment receive the recommended audit policy settings for Windows XP based computers. You can configure the Audit policy settings in Windows Vista at the following location in the Group Policy Object Editor: Computer Configuration\Windows Settings\Security Settings \Local Policies\Audit Policy

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits

setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

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, set the following Group Policy setting to `Success, Failure`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit
Policy\Audit logon 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.

1.1.1.2.2.5 Set 'Audit process tracking' to 'No Auditing' (Scored)

Profile Applicability:

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

Description:

This policy setting determines whether to audit detailed tracking information for events such as program activation, process exit, handle duplication, and indirect object access. Enabling Audit process tracking will generate a large number of events, so typically it is set to No Auditing. However, this setting can provide a great benefit during an incident response from the detailed log of the processes started and the time when they were launched.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

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, set the following Group Policy setting to `No Auditing`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit
Policy\Audit process tracking
```

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.

1.1.1.2.2.6 Set 'Audit account management' to 'Success, Failure' (Scored)

Profile Applicability:

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

Description:

This policy setting determines whether to audit each account management event on a computer. Examples of account management events include: . A user account or group is created, changed, or deleted. . A user account is renamed, disabled, or enabled. . A password is set or changed. Organizations need to be able to determine who creates, modifies, or deletes both domain and local accounts. Unauthorized changes could indicate mistaken changes made by an administrator who does not understand how to follow organizational policies, but could also indicate a deliberate attack. The following table includes the important security events that this policy setting records in the Security log. These event IDs can be useful when you want to create custom alerts to monitor any software suite, such as MOM. Most operational management software can be customized with scripts to capture or flag events that are based on these event IDs. Table 4.4 Account Management Events Event ID Event description 624 A user account was created. 627 A user password was changed. 628 A user password was set. 630 A user account was deleted. 631 A global group was created. 632 A member was added to a global group. 633 A member was removed from a global group. 634 A global group was deleted. 635 A new local group was created. 636 A member was added to a local group. 637 A member was removed from a local group. 638 A local group was deleted. 639 A local group account was changed. 641 A global group account was changed. 642 A user account was changed. 643 A domain policy was modified. 644 A user account was automatically locked. 645 A computer account was created. 646 A computer account was changed. 647 A computer account was deleted. 648 A local security group with security disabled was created. Note: SECURITY_DISABLED in the formal name means that this group cannot be used to grant permissions in access checks. 649 A local security group with security disabled was changed. 650 A member was added to a security-disabled local security group. 651 A member was removed from a security-disabled local security group. 652 A security-disabled local group was deleted. 653 A security-disabled global group was created. 654 A security-disabled global group was changed. 655 A member was added to a security-disabled global group. 656 A member was removed from a security-disabled global group. 657 A security-disabled global group was deleted. 658 A security-enabled universal group was created. 659 A security-enabled universal group was changed. 660 A member was added to a security-enabled universal group. 661 A member was removed from a security-enabled universal group. 662 A security-enabled universal group was deleted. 663 A security-disabled universal group was created. 664 A security-disabled universal group was changed. 665 A member was added to a security-disabled universal group. 666 A member was removed from a security-disabled universal group. 667 A security-disabled universal group was deleted. 668 A group type was changed. 684 The security descriptor of administrative group members was set. Note: Every 60 minutes on a domain controller, a background thread searches all members of administrative groups (such as domain, enterprise, and schema

administrators) and applies a fixed security descriptor on them. This event is logged. 685 Name of an account was changed.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

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, set the following Group Policy setting to `Success, Failure`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit
Policy\Audit 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.

1.1.1.2.2.7 Set 'Audit policy change' to 'Success' (Scored)

Profile Applicability:

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

Description:

This policy setting determines whether to audit every incident of a change to user rights assignment policies, Windows Firewall policies, Trust policies, or changes to the Audit policy itself. The recommended settings would let you see any account privileges that an attacker attempts to elevate for example, by adding the Debug programs privilege or the Back up files and directories privilege.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

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, set the following Group Policy setting to `Success`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit
Policy\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.

1.1.1.2.2.8 Set 'Audit system events' to 'Success' (Scored)

Profile Applicability:

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

Description:

This policy setting is very important because it allows you to monitor system events that succeed and fail, and provides a record of these events that may help determine instances of unauthorized system access. System events include starting or shutting down computers in your environment, full event logs, or other security-related events that affect the entire system.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

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, set the following Group Policy setting to `Success`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit
Policy\Audit 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.

1.1.1.2.2.9 Set 'Audit privilege use' to 'Failure' (Scored)

Profile Applicability:

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

Description:

This policy setting determines whether to audit each instance of a user exercising a user right. If you configure this value to Success, an audit entry is generated each time that a user right is exercised successfully. If you configure this value to Failure, an audit entry is generated each time that a user right is exercised unsuccessfully. This policy setting can generate a very large number of event records.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

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, set the following Group Policy setting to `Failure`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit
Policy\Audit 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.

1.1.1.2.2.10 Configure 'Audit object access' (Not Scored)

Profile Applicability:

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

Description:

Earlier security GPOs from Microsoft include settings that configure the audit categories in previous versions of Windows. These earlier GPOs do not apply to computers running Windows Vista. The GPOs intended for use in enterprise environments have been designed to work with Windows XP-based computers. Settings for audit categories are included in these GPOs so that computers running Windows XP in your environment receive the recommended audit policy settings for Windows XP based computers. You can configure the Audit policy settings in Windows Vista at the following location in the Group Policy Object Editor: Computer Configuration\Windows Settings\Security Settings \Local Policies\Audit Policy

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events

are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

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

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit
Policy\Audit object 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.

1.1.1.2.3 User Rights Assignment

1.1.1.2.3.1 Set 'Allow log on through Terminal Services' to 'Administrators' (Scored)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This policy setting determines which users or groups have the right to log on as a Terminal Services client. Remote desktop users require this user right. 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. When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.

Rationale:

Any account with the Allow log on through Terminal 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 implement the recommended configuration state, set the following Group Policy setting to `Administrators`.

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

Impact:

Removal of the Allow log on through Terminal 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.

1.1.1.2.3.2 Set 'Allow log on through Terminal Services' to 'Administrators, Remote desktop Users' (Scored)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy setting determines which users or groups have the right to log on as a Terminal Services client. Remote desktop users require this user right. 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. When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.

Rationale:

Any account with the Allow log on through Terminal 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 implement the recommended configuration state, set the following Group Policy setting to `Administrators, Remote desktop Users`.

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

Impact:

Removal of the Allow log on through Terminal 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.

1.1.1.2.3.3 Set 'Take ownership of files or other objects' 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. When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.

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 denial of service (DoS) condition.

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, set the following Group Policy setting to `Administrators`.

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

Impact:

None. This is the default configuration.

1.1.1.2.3.4 Set 'Enable computer and user accounts to be trusted for delegation' to 'Administrators' (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. When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.

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 implement the recommended configuration state, set the following Group Policy setting to `Administrators`.

```
Computer Configuration\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 configuration.

1.1.1.2.3.5 Configure 'Enable computer and user accounts to be trusted for delegation' (Not 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. When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.

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 for your organization.

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\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 configuration.

1.1.1.2.3.6 Set 'Remove computer from docking station' to 'Administrators' (Scored)

Profile Applicability:

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

Description:

This policy setting allows the user of a portable computer to click Eject PC on the Start menu to undock the computer. When configuring a user right in the SCM enter a comma

delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.

Rationale:

Anyone who has the Remove computer from docking station user right can log on and then remove a portable computer from its docking station. If this setting is not defined, it has the same effect as if everyone was granted this right. However, the value of implementing this countermeasure is reduced by the following factors: . If attackers can restart the computer, they could remove it from the docking station after the BIOS starts but before the operating system starts. . This setting does not affect servers, because they typically are not installed in docking stations. . An attacker could steal the computer and the docking station together.

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, set the following Group Policy setting to `Administrators`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Remove computer from docking station
```

Impact:

In Windows XP and Windows Server 2003 only members of the local Administrators and Power Users groups are granted this right by default. In later versions of Windows members of the local Administrators and Users groups have this right by default. Other user accounts must be explicitly granted the right as necessary. If your organization's users are not members of these groups on their portable computers, they will be unable to remove their own portable computers from their docking stations without shutting them down first. Therefore, on Windows XP, you may want to assign the Remove computer from docking station privilege to the local Users group for portable computers.

1.1.1.2.3.7 Configure 'Create permanent shared objects' (Not 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. When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.

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 for your organization.

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

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

Impact:

None. This is the default configuration.

1.1.1.2.3.8 Set 'Debug programs' 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. Note Microsoft released several security updates in October 2003 that used a version of Update.exe that required the administrator to have the Debug programs user right. Administrators who did not have this user right were unable to install these security updates until they reconfigured their user rights. This is not typical

behavior for operating system updates. For more information, see Knowledge Base article 830846: Windows Product Updates may stop responding or may use most or all the CPU resources. When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.

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. The value of removing this user right from members of the Administrators group is diminished by the fact that a malicious user who has administrative privileges can bypass the countermeasure by launching processes under the Local System account.

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, set the following Group Policy setting to `Administrators`.

```
Computer Configuration\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. If you do revoke this privilege from all accounts and 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 privilege; if it does not have it, Windows Clustering will fail. For additional information about how to configure Windows Clustering in conjunction with computer hardening, see article 891597, How to apply more restrictive security settings on a Windows Server 2003based cluster server, in the Microsoft Knowledge Base (http://go.microsoft.com/fwlink/?LinkId=100746). 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. Task Manager will not be able to manage processes owned by other accounts. Also, some older versions of Update.exe (which is used to install Windows product updates) require the account that applies the update to have this user right. If you install one of the patches that uses this version of Update.exe, the computer could become unresponsive. For more information, see article 830846, Windows Product Updates may stop responding or may use most or all the CPU resources, in the Microsoft Knowledge Base (http://go.microsoft.com/fwlink/?LinkId=100747).

1.1.1.2.3.9 Configure 'Load and unload device drivers' (Not 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. When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.

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 for your organization.

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\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.

1.1.1.2.3.10 Set 'Adjust memory quotas for a process' 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. When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.

Rationale:

A user with the Adjust memory quotas for a process privilege 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 implement the recommended configuration state, set the following Group Policy setting to `Administrators, LOCAL SERVICE, NETWORK SERVICE`.

```
Computer Configuration\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. IIS requires that this privilege be explicitly assigned to the IWAM_<ComputerName>, Network Service, and Service accounts. 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.

1.1.1.2.3.11 Configure 'Generate security audits' (Not 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. When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.

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 for your organization.

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

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

Impact:

None. This is the default configuration.

1.1.1.2.3.12 Set 'Shut down the system' 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. When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.

Rationale:

The ability to shut down domain controllers 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. 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 SingleMaster Operations (FSMO) roles, you can disable key domain functionality, such as processing logons for new passwords 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 implement the recommended configuration state, set the following Group Policy setting to `Administrators`.

```
Computer Configuration\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.

1.1.1.2.3.13 Configure 'Increase scheduling priority' (Not 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. When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.

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 denial of service (DoS) condition.

Audit:

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

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

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

Impact:

None. This is the default configuration.

1.1.1.2.3.14 Set 'Replace a process level token' 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. When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.

Rationale:

User 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 implement the recommended configuration state, set the following Group Policy setting to `LOCAL SERVICE, NETWORK SERVICE`.

```
Computer Configuration\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 optional components such as ASP.NET or IIS, you may need to assign the Replace a process level token privilege to additional accounts. For example, IIS requires that the Service, Network Service, and IWAM_<ComputerName> accounts be explicitly granted this user right.

1.1.1.2.3.15 Configure 'Add workstations to domain' (Not Scored)

Profile Applicability:

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

Description:

This policy setting specifies which users can add computer workstations to a specific 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 they have been assigned the Add workstations to a domain user right. By default, all users in the Authenticated Users group 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. 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. When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.

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 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 for your organization.

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\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 computers unless they are removed from and re-added to the domain.

1.1.1.2.3.16 Configure 'Change the system time' (Not 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. When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers. 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 for your organization.

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\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.

1.1.1.2.3.17 Configure 'Restore files and directories' (Not 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 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. When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.

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 are used to back up data.

Audit:

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

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\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.

1.1.1.2.3.18 Configure 'Create a token object' (Not 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. When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.

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 denial of service (DoS) condition.

Audit:

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

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

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

Impact:

None. This is the default configuration.

1.1.1.2.3.19 Configure 'Synchronize directory service data' (Not Scored)

Profile Applicability:

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

Description:

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 for your organization.

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights
Assignment\Synchronize directory service data
```

Impact:

None. This is the default configuration.

1.1.1.2.3.20 Set 'Profile system performance' to 'Administrators' (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. When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.

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 implement the recommended configuration state, set the following Group Policy setting to `Administrators`.

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

Impact:

None. This is the default configuration.

1.1.1.2.3.21 Configure 'Access this computer from the network' (Not Scored)

Profile Applicability:

- Level 1 - Domain Controller
- 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+). When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.

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 in the group will be able to read the files in those shared folders. However, this situation is unlikely for new installations of recent versions of Windows, because the default share and NTFS permissions 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 and later versions of the Windows operating system.

Audit:

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

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\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 it is recommended that it is assigned to the 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.

1.1.1.2.3.22 Set 'Profile single process' 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. When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.

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 implement the recommended configuration state, set the following Group Policy setting to `Administrators`.

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

Impact:

If you remove the Profile single process user right from the Power Users group or other accounts, you could limit the abilities of users who are assigned to specific administrative

roles in your environment. You should ensure that delegated tasks will not be negatively affected.

1.1.1.2.3.23 Configure 'Impersonate a client after authentication' (Not Scored)

Profile Applicability:

- Level 1 - Domain Controller
- 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. When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.

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 for your organization.

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\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 optional components such as ASP.NET or IIS, you may need to assign the Impersonate a client after authentication user right to additional accounts that are required by those components, such as IUSR_<ComputerName>, IIS_WPG, ASP.NET or IWAM_<ComputerName>.

1.1.1.2.3.24 Set 'Create a pagefile' 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. When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.

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 implement the recommended configuration state, set the following Group Policy setting to `Administrators`.

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

Impact:

None. This is the default configuration.

1.1.1.2.3.25 Set 'Deny log on as a batch job' to '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. The Deny log on as a batch job user right overrides 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. When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.

Rationale:

Accounts that have the Deny 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 implement the recommended configuration state, set the following Group Policy setting to `Guests`.

```
Computer Configuration\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.

1.1.1.2.3.26 Set 'Deny log on through Terminal Services' to 'Guests' (Scored)

Profile Applicability:

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

Description:

This policy setting determines whether users can log on as Terminal Services 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. When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.

Rationale:

Any account with the right to log on through Terminal 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 implement the recommended configuration state, set the following Group Policy setting to `Guests`.

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

Impact:

If you assign the Deny log on through Terminal 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 Terminal Services or Remote Assistance. You should confirm that delegated tasks will not be negatively impacted.

1.1.1.2.3.27 Configure 'Act as part of the operating system' (Not 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. When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.

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 for your organization.

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\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.

1.1.1.2.3.28 Configure 'Back up files and directories' (Not 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. When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.

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 for your organization.

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\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.

1.1.1.2.3.29 Set 'Log on as a service' to 'NETWORK SERVICE' (Scored)

Profile Applicability:

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

Description:

This policy setting allows accounts to launch network services or to register a process as a service running on the system. This user right should be restricted on any computer in a high security environment, but because many applications may require this privilege, it should be carefully evaluated and tested before configuring it in an enterprise environment. On Windows Vista based computers, no users or groups have this privilege by default. When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.

Rationale:

Log on as a service is a powerful user right because it allows accounts to launch network services or services that run continuously on a computer, even when no one is logged on to the console. The risk is reduced by the fact that only users with administrative privileges can install and configure services. An attacker who has already attained that level of access could configure the service to run with the Local System account.

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, set the following Group Policy setting to `NETWORK SERVICE`.

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

Impact:

On most computers, this is the default configuration and there will be no negative impact. However, if you have installed optional components such as ASP.NET or IIS, you may need to assign the Log on as a service user right to additional accounts that are required by those

components. IIS requires that this user right be explicitly granted to the ASPNET user account.

1.1.1.2.3.30 Set 'Deny access to this computer from the network' to 'ANONYMOUS LOGON, Guests' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- 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. When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.

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 implement the recommended configuration state, set the following Group Policy setting to `ANONYMOUS LOGON, Guests`.

```
Computer Configuration\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.

1.1.1.2.3.31 Configure 'Perform volume maintenance tasks' (Not 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. When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.

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 denial of service (DoS) condition.

Audit:

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

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

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

Impact:

None. This is the default configuration.

1.1.1.2.3.32 Configure 'Deny log on locally' (Not 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. Important: If you apply this security policy to the Everyone group, no one will be able to log on locally. When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.

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 for your organization.

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\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.

1.1.1.2.3.33 Set 'Allow log on locally' 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 or IIS also require this user right. The Guest account is assigned this user right by default. Although this account is disabled by default, it is recommended that you enable this setting through Group Policy. However, this user right should generally be restricted to the Administrators and Users groups. Assign this user right to the Backup Operators group if your organization requires that they have this capability. When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.

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 implement the recommended configuration state, set the following Group Policy setting to `Administrators`.

```
Computer Configuration\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. If you have installed optional components such as ASP.NET or Internet Information Services, you may need to assign Allow log on locally user right to additional accounts that are required by those components. IIS requires that this user right be assigned to the IUSR_<ComputerName> account. You should confirm that delegated activities will not be adversely affected by any changes that you make to the Allow log on locally user rights assignments.

1.1.1.2.3.34 Configure 'Create global objects' (Not 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. When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.

Rationale:

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.

Audit:

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

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

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

Impact:

None. This is the default configuration.

1.1.1.2.3.35 Configure 'Bypass traverse checking' (Not Scored)

Profile Applicability:

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

Description:

This policy setting allows users who do not have the Traverse Folder access permission to pass through folders when they browse an object path in the NTFS file system or the

registry. This user right does not allow users to list the contents of a folder. When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.

Rationale:

The default configuration for the Bypass traverse checking setting is to allow all users, including the Everyone group, to bypass traverse checking. Permissions to files and folders are controlled though appropriate configuration of file system access control lists (ACLs), as the ability to traverse the folder does not provide any read or write permissions to the user. The only scenario in which the default configuration could lead to a mishap would be if the administrator who configures permissions does not understand how this policy setting works. For example, the administrator might expect that users who are unable to access a folder will be unable to access the contents of any child folders. Such a situation is unlikely, and therefore this vulnerability presents little risk.

Audit:

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

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights
Assignment\Bypass traverse checking
```

Impact:

The Windows operating systems, as well as many applications, were designed with the expectation that anyone who can legitimately access the computer will have this user right. Therefore, we recommend that you thoroughly test any changes to assignments of the Bypass traverse checking user right before you make such changes to production systems. In particular, IIS requires this user right to be assigned to the Network Service, Local Service, IIS_WPG, IUSR_<ComputerName>, and IWAM_<ComputerName> accounts. (It must also be assigned to the ASPNET account through its membership in the Users group.) We recommend that you leave this policy setting at its default configuration.

1.1.1.2.3.36 Configure 'Deny log on as a service' (Not 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 policy setting supersedes the Log on as a service policy setting if an account is subject to both policies. Note: This security setting does not apply to the System, Local Service, or Network Service accounts. When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.

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 for your organization.

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\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.

1.1.1.2.3.37 Set 'Manage auditing and security log' to 'Administrators' (Scored)

Profile Applicability:

- Level 1 - Domain Controller

- 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. When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.

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 implement the recommended configuration state, set the following Group Policy setting to `Administrators`.

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

Impact:

None. This is the default configuration.

1.1.1.2.3.38 Configure 'Lock pages in memory' (Not 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. When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.

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 denial of service (DoS) condition.

Audit:

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

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

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

Impact:

None. This is the default configuration.

1.1.1.2.3.39 Configure 'Force shutdown from a remote system' (Not Scored)

Profile Applicability:

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

Description:

This policy setting allows users to shut down Windows Vista based 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. When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.

Rationale:

Any user who can shut down a computer could cause a denial of service (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 for your organization.

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\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.

1.1.1.2.3.40 Set 'Modify firmware environment values' 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. When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.

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 denial of service (DoS) condition.

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, set the following Group Policy setting to `Administrators`.

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

Impact:

None. This is the default configuration.

1.1.1.2.3.41 Configure 'Log on as a batch job' (Not Scored)

Profile Applicability:

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

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. When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.

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 for your organization.

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
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.

1.1.1.3 Event Log

1.1.1.3.1 Set 'Retention method for system log' to 'Overwrites events as needed' (Scored)

Profile Applicability:

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

Description:

This policy setting determines the wrapping method for the System log. It is imperative that the System log is archived regularly if historical events are desirable for either forensics or troubleshooting purposes. Overwriting events as needed ensures that the log always stores the most recent events, although this configuration could result in a loss of historical data.

Rationale:

If you significantly increase the number of objects to audit in your organization, there is a risk that the Security log will reach its capacity and force the computer to shut down. If such a shutdown occurs, the computer will be unusable until an administrator clears the Security log. To prevent such a shutdown, you can disable the Audit: Shut down system immediately if unable to log security audits setting that is described in Security Options and then increase the Security log size. If you set the Event log retention method to Manual or Overwrite events by days, it is possible for important recent events to not be recorded or for a DoS attack to occur.

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, set the following Group Policy setting to `WhenNeeded`.

```
Computer Configuration\Windows Settings\Security Settings\Event Log\Retention method
for system log
```

Impact:

When event logs fill to capacity, they will stop recording information unless the retention method is set so that the computer can overwrite the oldest entries with the most recent ones.

1.1.1.3.2 Set 'Maximum application log size' to '16384' (Scored)

Profile Applicability:

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

Description:

This policy setting specifies the maximum size of the Application event log. In Windows Vista and Windows Server 2008 this setting has been replaced by another called System, located at Computer Configuration\Administrative Templates\Windows Components\Event Log Service. If both this setting and the new one are configured the setting at Computer Configuration\Administrative Templates\Windows Components\Event Log Service will take precedence.

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.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `16384`.

```
Computer Configuration\Windows Settings\Security Settings\Event Log\Maximum
application log size
```

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 Operations Manager (MOM) 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.

1.1.1.3.3 Set 'Retention method for security log' to 'Overwrites events as needed' (Scored)

Profile Applicability:

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

Description:

This policy setting determines the wrapping method for the Security log. It is imperative that the Security log is archived regularly if historical events are desirable for either forensics or troubleshooting purposes. Overwriting events as needed ensures that the log always stores the most recent events, although this configuration could result in a loss of historical data.

Rationale:

If you significantly increase the number of objects to audit in your organization, there is a risk that the Security log will reach its capacity and force the computer to shut down. If such a shutdown occurs, the computer will be unusable until an administrator clears the

Security log. To prevent such a shutdown, you can disable the Audit: Shut down system immediately if unable to log security audits setting that is described in Security Options and then increase the Security log size. If you set the Event log retention method to Manual or Overwrite events by days, it is possible for important recent events to not be recorded or for a DoS attack to occur.

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, set the following Group Policy setting to `WhenNeeded`.

```
Computer Configuration\Windows Settings\Security Settings\Event Log\Retention method
for security log
```

Impact:

When event logs fill to capacity, they will stop recording information unless the retention method is set so that the computer can overwrite the oldest entries with the most recent ones.

1.1.1.3.4 Set 'Maximum system log size' to '16384' (Scored)

Profile Applicability:

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

Description:

This policy setting specifies the maximum size of the System event log. In Windows Vista and Windows Server 2008 this setting has been replaced by another called System, located at Computer Configuration\Administrative Templates\Windows Components\Event Log Service. If both this setting and the new one are configured the setting at Computer Configuration\Administrative Templates\Windows Components\Event Log Service will take precedence.

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.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `16384`.

```
Computer Configuration\Windows Settings\Security Settings\Event Log\Maximum system log size
```

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 Operations Manager (MOM) 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.

1.1.1.3.5 Set 'Maximum security log size' to '81920' (Scored)

Profile Applicability:

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

Description:

This policy setting specifies the maximum size of the System event log. In Windows Vista and Windows Server 2008 this setting has been replaced by another called System, located at Computer Configuration\Administrative Templates\Windows Components\Event Log Service. If both this setting and the new one are configured the setting at Computer Configuration\Administrative Templates\Windows Components\Event Log Service will take precedence.

Rationale:

If you significantly increase the number of objects to audit in your organization, there is a risk that the Security log will reach its capacity and force the computer to shut down if you enabled the Audit: Shut down system immediately if unable to log security audits setting. If such a shutdown occurs, the computer will be unusable until an administrator clears the Security log. To prevent such a shutdown, you can disable the Audit: Shut down system immediately if unable to log security audits setting that is described in Chapter 5, "Security Options," and increase the Security log size. Alternatively, you can configure automatic log rotation as described in the Microsoft Knowledge Base article "The event log stops logging events before reaching the maximum log size" at http://support.microsoft.com/default.aspx?kbid=312571.

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, set the following Group Policy setting to `81920`.

```
Computer Configuration\Windows Settings\Security Settings\Event Log\Maximum security
log size
```

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 Operations Manager (MOM) 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.

1.1.1.3.6 Set 'Retention method for application log' to 'Overwrites events as needed' (Scored)

Profile Applicability:

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

Description:

This policy setting determines the wrapping method for the Application log. It is imperative that the Application log is archived regularly if historical events are desirable for either forensics or troubleshooting purposes. Overwriting events as needed ensures that the log always stores the most recent events, although this configuration could result in a loss of historical data.

Rationale:

If you significantly increase the number of objects to audit in your organization, there is a risk that the Security log will reach its capacity and force the computer to shut down. If such a shutdown occurs, the computer will be unusable until an administrator clears the Security log. To prevent such a shutdown, you can disable the Audit: Shut down system immediately if unable to log security audits setting that is described in Security Options and then increase the Security log size. If you set the Event log retention method to Manual or Overwrite events by days, it is possible for important recent events to not be recorded or for a DoS attack to occur.

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, set the following Group Policy setting to `WhenNeeded`.

```
Computer Configuration\Windows Settings\Security Settings\Event Log\Retention method
for application log
```

Impact:

When event logs fill to capacity, they will stop recording information unless the retention method is set so that the computer can overwrite the oldest entries with the most recent ones.

1.1.1.3.7 Configure 'Retain system log' (Not Scored)

Profile Applicability:

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

Description:

This setting turns on and off the option to retain the system log and works in conjunction with the Retention method for system log setting.

Rationale:

If you archive the log at scheduled intervals: 1. Open the Properties dialog box for this policy setting. 2. Specify the appropriate number of days in the Retain application log setting. 3. Select Overwrite events by days for the event log retention method. Also, ensure that the maximum log size is large enough to accommodate the interval.

Audit:

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

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Windows Settings\Security Settings\Event Log\Retain system log
```

Impact:

None. This is the default configuration.

1.1.1.3.8 Configure 'Retain security log' (Not Scored)

Profile Applicability:

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

Description:

This setting is the toggle setting to retain the security log and works with the Retention method for the security log setting.

Rationale:

If you archive the log at scheduled intervals: 1. Open the Properties dialog box for this policy setting. 2. Specify the appropriate number of days in the Retain application log setting. 3. Select Overwrite events by days for the event log retention method. Also, ensure that the maximum log size is large enough to accommodate the interval.

Audit:

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

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Windows Settings\Security Settings\Event Log\Retain security log
```

Impact:

None. This is the default configuration.

1.1.1.3.9 Configure 'Retain application log' (Not Scored)

Profile Applicability:

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

Description:

This setting is the toggle setting to retain the application log and works in conjunction with the retention method for application logs setting.

Rationale:

If you archive the log at scheduled intervals: 1. Open the Properties dialog box for this policy setting. 2. Specify the appropriate number of days in the Retain application log setting. 3. Select Overwrite events by days for the event log retention method. Also, ensure that the maximum log size is large enough to accommodate the interval.

Audit:

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

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Windows Settings\Security Settings\Event Log\Retain application log
```

Impact:

None. This is the default configuration.

1.2 Administrative Templates

1.2.1 Network

1.2.1.1 Network Connections

1.2.1.1.1 Windows Firewall

1.2.1.1.1.1 Standard Profile

1.2.1.1.1.1.1 Configure 'Windows Firewall: Allow ICMP exceptions' (Not Scored)

Profile Applicability:

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

Description:

This policy setting defines the set of Internet Control Message Protocol (ICMP) message types that Windows Firewall allows. Utilities can use ICMP messages to determine the status of other computers. For example, Ping uses the echo request message.

Rationale:

Many attacker tools take advantage of computers that accept ICMP message types and use these messages to mount a variety of attacks.

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\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile\IcmpSet
tings:AllowOutboundParameterProblem
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Network\Network Connections\Windows
Firewall\Standard Profile\Windows Firewall: Allow ICMP exceptions
```

Impact:

If you configure the Windows Firewall: Allow ICMP exceptions setting to Enabled, you must specify which ICMP message types Windows Firewall allows the computer to send or receive. When you configure this policy setting to Disabled, Windows Firewall blocks all unsolicited inbound ICMP message types and the listed outbound ICMP message types. As a result, utilities that rely on ICMP may fail. Some applications require some ICMP messages in order to function properly. Also, ICMP messages are used to estimate network performance when Group Policy is downloaded and processed; if ICMP messages are blocked, Group Policy may not be applied to affected systems. Note If any policy setting opens TCP port 445, Windows Firewall allows inbound ICMP echo request messages (such as those sent by the Ping utility), even if the Windows Firewall: Allow ICMP exceptions policy setting would block them. Policy settings that can open TCP port 445 include Windows Firewall: Allow inbound file and printer sharing exception, Windows Firewall: Allow inbound remote administration exception, and Windows Firewall: Define inbound port exceptions.

1.2.1.1.1.1.2 Configure 'Windows Firewall: Define inbound port exceptions' (Not Scored)

Profile Applicability:

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

Description:

Microsoft recommends that you avoid the use of this setting, unless required by your environment and your organization's business requirements. The Windows Firewall port exceptions list should be defined by Group Policy, which allows you to centrally manage and deploy your port exceptions and ensure that local administrators do not create less secure settings.

Rationale:

Granting port exceptions could expose the computer to network-based attacks, however not allowing any exceptions is likely to break some applications such as computer management tools

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\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile\GloballyOpenPorts:Enabled
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Network\Network Connections\Windows Firewall\Standard Profile\Windows Firewall: Define inbound port exceptions
```

Impact:

If you enable the Windows Firewall: Define inbound port exceptions setting, you can view and change the port exceptions list that is defined by Group Policy. To view and modify the port exceptions list, configure the setting to Enabled and then click the Show button. Note that if you type an invalid definition string, Windows Firewall adds it to the list without

checking for errors, which means that you can accidentally create multiple entries for the same port with Scope or Status values that conflict. If you disable the Windows Firewall: Define inbound port exceptions setting, the port exceptions list that is defined by Group Policy is deleted but other settings can continue to open or block ports. Also, if a local port exceptions list exists, it is ignored unless you enable the Windows Firewall: Allow local port exceptions setting. Note If any policy setting opens TCP port 445, Windows Firewall allows inbound ICMP echo request messages (such as those sent by the Ping utility), even if the Windows Firewall: Allow ICMP exceptions policy setting would block them. Policy settings that can open TCP port 445 include Windows Firewall: Allow inbound file and printer sharing exception, Windows Firewall: Allow inbound remote administration exception, and Windows Firewall: Define inbound port exceptions.

1.2.1.1.1.1.3 Configure 'Windows Firewall: Prohibit unicast response to multicast or broadcast requests' (Not Scored)

Profile Applicability:

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

Description:

This policy setting helps prevent a computer from receiving unicast responses to its outgoing multicast or broadcast messages.

Rationale:

Typically, you would not want to receive unicast responses to multicast or broadcast messages. Such responses can indicate a denial of service (DoS) attack or an attempt to probe a known computer.

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\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile:Disable
UnicastResponsesToMulticastBroadcast
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Network\Network Connections\Windows
Firewall\Standard Profile\Windows Firewall: Prohibit unicast response to multicast or
broadcast requests
```

Impact:

Note This policy setting has no effect if the unicast message is a response to a DHCP broadcast message that is sent by the computer. Windows Firewall always permits those DHCP responses. However, this policy setting can interfere with the NetBIOS messages that detect name conflicts.

1.2.1.1.1.1.4 Configure 'Windows Firewall: Allow local program exceptions' (Not Scored)

Profile Applicability:

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

Description:

Microsoft recommends that you avoid the use of this setting, unless required by your environment and your organization's business requirements. This policy setting controls whether administrators can use the Windows Firewall component in Control Panel to define a local program exceptions list.

Rationale:

Granting program exceptions could expose the computer to network-based attacks, however not allowing any exceptions is likely to break some applications such as computer management tools

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\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile\Authori
zedApplications:AllowUserPrefMerge
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Network\Network Connections\Windows
Firewall\Standard Profile\Windows Firewall: Allow local program exceptions
```

Impact:

If you disable this policy setting, administrators will not be able to define a local program exceptions list; also, this configuration ensures that program exceptions only come from Group Policy. If this policy setting is enabled, local administrators are allowed to use Control Panel to define program exceptions locally. For enterprise client computers, there may be conditions that justify local program exceptions. These conditions may include applications that were not analyzed when the organization's firewall policy was created or new applications that require nonstandard port configuration. If you choose to enable the Windows Firewall: Allow local program exceptions setting for such situations, remember that the attack surface of the affected computers is increased.

1.2.1.1.1.1.5 Configure 'Windows Firewall: Allow inbound remote administration exception' (Not Scored)

Profile Applicability:

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

Description:

Many organizations take advantage of remote computer administration in their daily operations. To provide flexibility for remote administration, the Windows Firewall: Allow inbound remote administration exception setting is available. If you enable this setting, computers in your environment should accept remote administration requests from as few computers as possible. To maximize the protection provided by Windows Firewall, make sure to specify only the necessary IP addresses and subnets of computers that are used for remote administration.

Rationale:

Some attacks have exploited the ports that are typically used by remote administration programs; Windows Firewall can help block these ports.

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\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile\RemoteAdminSettings:Enabled
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Network\Network Connections\Windows Firewall\Standard Profile\Windows Firewall: Allow inbound remote administration exception
```

Impact:

If this policy setting is enabled, the computer can receive the unsolicited incoming messages that are associated with remote administration on TCP ports 135 and 445. This policy setting also allows Svchost.exe and Lsass.exe to receive unsolicited incoming messages and allows hosted services to open additional dynamically-assigned ports, typically in the range of 1024 to 1034 but potentially anywhere from 1024 to 65535. If you enable this policy setting, you need to specify the IP addresses or subnets from which these incoming messages are allowed. If you configure the Windows Firewall: Allow inbound remote administration exception setting to Disabled, Windows Firewall makes none of the described exceptions. The impact of configuring this policy setting to Disabled may be unacceptable to many organizations because many remote administration tools and tools that scan for vulnerabilities will fail.

1.2.1.1.1.1.6 Configure 'Windows Firewall: Allow inbound Remote Desktop exceptions' (Not Scored)

Profile Applicability:

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

Description:

Many organizations use Remote Desktop connections in their normal troubleshooting procedures or operations. To provide flexibility for remote administration, the Windows Firewall: Allow inbound Remote Desktop exceptions setting is available.

Rationale:

Some attacks have exploited the ports that are typically used by Remote Desktop.

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\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile\Service
s\RemoteDesktop:Enabled
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Network\Network Connections\Windows
Firewall\Standard Profile\Windows Firewall: Allow inbound Remote Desktop exceptions
```

Impact:

If you enable this policy setting, Windows Firewall opens TCP port 3389 for inbound connections. You must also specify the IP addresses or subnets from which these inbound messages are allowed. If you disable this policy setting, Windows Firewall blocks this port and prevents the computer from receiving Remote Desktop requests. If an administrator adds this port to a local port exceptions list in an attempt to open it, Windows Firewall does not open the port. Computers in your environment should accept Remote Desktop requests from as few computers as possible.

1.2.1.1.1.1.7 Configure 'WF_IcmpSettings_AllowOutboundSourceQuench' (Not Scored)

Profile Applicability:

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

Description:

If you configure the Windows Firewall: Allow ICMP exceptions setting to Enabled, you must specify which ICMP message types Windows Firewall allows the computer to send or receive.

Rationale:

See parent information.

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\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile\IcmpSet
tings:AllowOutboundParameterProblem
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Network\Network Connections\Windows
Firewall\Standard Profile\WF_IcmpSettings_AllowOutboundSourceQuench
```

Impact:

See parent information.

1.2.1.1.1.1.8 Configure 'WF_IcmpSettings_AllowOutboundParameterProblem' (Not Scored)

Profile Applicability:

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

Description:

If you configure the Windows Firewall: Allow ICMP exceptions setting to Enabled, you must specify which ICMP message types Windows Firewall allows the computer to send or receive.

Rationale:

See parent information.

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\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile\IcmpSet
tings:AllowOutboundParameterProblem
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Network\Network Connections\Windows
Firewall\Standard Profile\WF_IcmpSettings_AllowOutboundParameterProblem
```

Impact:

See parent information.

1.2.1.1.1.1.9 Configure 'Windows Firewall: Allow inbound UPnP framework exceptions' (Not Scored)

Profile Applicability:

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

Description:

This policy setting allows a computer to receive unsolicited Plug and Play messages that are sent by network devices, such as routers with built-in firewalls. To receive these messages, Windows Firewall opens TCP port 2869 and UDP port 1900.

Rationale:

Blocking UPnP network traffic effectively reduces the attack surface of computers in your environment.

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\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile\Service
s\UPnPFramework:Enabled
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Network\Network Connections\Windows
Firewall\Standard Profile\Windows Firewall: Allow inbound UPnP framework exceptions
```

Impact:

If you enable the Windows Firewall: Allow inbound UPnP framework exceptions setting, Windows Firewall opens these ports so that the computer can receive Plug and Play messages. You must specify the IP addresses or subnets from which these inbound messages are allowed. If you disable this policy setting, Windows Firewall blocks these ports and prevents the computer from receiving Plug and Play messages.

1.2.1.1.1.1.10 Configure 'WF_IcmpSettings_AllowInboundMaskRequest' (Not Scored)

Profile Applicability:

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

Description:

If you configure the Windows Firewall: Allow ICMP exceptions setting to Enabled, you must specify which ICMP message types Windows Firewall allows the computer to send or receive.

Rationale:

See parent information.

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\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile\IcmpSet
tings:AllowOutboundParameterProblem
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Network\Network Connections\Windows
Firewall\Standard Profile\WF_IcmpSettings_AllowInboundMaskRequest
```

Impact:

See parent information.

1.2.1.1.1.1.11 Configure 'WF_IcmpSettings_AllowRedirect' (Not Scored)

Profile Applicability:

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

Description:

If you configure the Windows Firewall: Allow ICMP exceptions setting to Enabled, you must specify which ICMP message types Windows Firewall allows the computer to send or receive.

Rationale:

See parent information.

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\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile\IcmpSet
tings:AllowOutboundParameterProblem
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Network\Network Connections\Windows
Firewall\Standard Profile\WF_IcmpSettings_AllowRedirect
```

Impact:

See parent information.

1.2.1.1.1.1.12 Configure 'WF_IcmpSettings_AllowOutboundDestinationUnreachable' (Not Scored)

Profile Applicability:

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

Description:

If you configure the Windows Firewall: Allow ICMP exceptions setting to Enabled, you must specify which ICMP message types Windows Firewall allows the computer to send or receive.

Rationale:

See parent information.

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\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile\IcmpSettings:AllowOutboundParameterProblem
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Network\Network Connections\Windows Firewall\Standard Profile\WF_IcmpSettings_AllowOutboundDestinationUnreachable
```

Impact:

See parent information.

1.2.1.1.1.1.13 Configure 'WF_IcmpSettings_AllowOutboundTimeExceeded' (Not Scored)

Profile Applicability:

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

Description:

If you configure the Windows Firewall: Allow ICMP exceptions setting to Enabled, you must specify which ICMP message types Windows Firewall allows the computer to send or receive.

Rationale:

See parent information.

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\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile\IcmpSet
tings:AllowOutboundParameterProblem
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Network\Network Connections\Windows
Firewall\Standard Profile\WF_IcmpSettings_AllowOutboundTimeExceeded
```

Impact:

See parent information.

1.2.1.1.1.1.14 Configure 'Windows Firewall: Allow inbound file and printer sharing exception' (Not Scored)

Profile Applicability:

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

Description:

This policy setting creates an exception that allows file and printer sharing. It configures Windows Firewall to open UDP ports 137 and 138 and TCP ports 139 and 445.

Rationale:

Enabling access to file and printer sharing could cause a user to unknowingly expose sensitive data. Additionally, there have been vulnerabilities in the resource sharing features that have been remotely exploitable.

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\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile\Service
s\FileAndPrint:Enabled
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Network\Network Connections\Windows
Firewall\Standard Profile\Windows Firewall: Allow inbound file and printer sharing
exception
```

Impact:

If you enable this policy setting, Windows Firewall opens these ports so that the computer can receive print jobs and requests for access to shared files. You must specify the IP addresses or subnets from which such messages are allowed. If you disable the Windows Firewall: Allow inbound file and printer sharing exception setting, Windows Firewall blocks these ports and prevents the computer from sharing files and printers. Note If any policy setting opens TCP port 445, Windows Firewall allows inbound ICMP echo request messages (such as those sent by the Ping utility), even if the Windows Firewall: Allow ICMP exceptions policy setting would block them. Policy settings that can open TCP port 445 include Windows Firewall: Allow inbound file and printer sharing exception, Windows Firewall: Allow inbound remote administration exception, and Windows Firewall: Define inbound port exceptions.

1.2.1.1.1.1.15 Configure 'Windows Firewall: Define inbound program exceptions' (Not Scored)

Profile Applicability:

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

Description:

Microsoft recommends that you use this setting, if appropriate to your environment and your organization's business requirements, to help protect end user computers. Some applications may need to open and use network ports that are not typically allowed by

Windows Firewall. The Windows Firewall: Define inbound program exceptions setting allows you to view and change the program exceptions list that is defined by Group Policy.

Rationale:

There is risk that inbound exceptions will be made to programs that have software vulnerabilities, however, if exceptions are not allowed then management programs and other useful applications will fail.

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\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile\Authori
zedApplications:Enabled
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Network\Network Connections\Windows
Firewall\Standard Profile\Windows Firewall: Define inbound program exceptions
```

Impact:

If this policy setting is Enabled you can view and change the program exceptions list. If you add a program to this list and set its status to Enabled, that program can receive unsolicited incoming messages on any port that it requests Windows Firewall to open, even if that port is blocked by another setting. If you configure this policy setting to Disabled, the program exceptions list that is defined by Group Policy is deleted. Note If you type an invalid definition string, Windows Firewall adds it to the list without checking for errors. Because the entry is not checked, you can add programs that you have not installed yet. You can also accidentally create multiple exceptions for the same program with Scope or Status values that conflict.

1.2.1.1.1.1.16 Configure 'WF_IcmpSettings_AllowInboundRouterRequest' (Not Scored)

Profile Applicability:

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

Description:

If you configure the Windows Firewall: Allow ICMP exceptions setting to Enabled, you must specify which ICMP message types Windows Firewall allows the computer to send or receive.

Rationale:

See parent information.

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\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile\IcmpSettings:AllowOutboundParameterProblem
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Network\Network Connections\Windows Firewall\Standard Profile\WF_IcmpSettings_AllowInboundRouterRequest
```

Impact:

See parent information.

1.2.1.1.1.1.17 Configure 'Windows Firewall: Allow local port exceptions' (Not Scored)

Profile Applicability:

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

Description:

The Windows Firewall port exceptions list should be defined by Group Policy, which allows you to centrally manage and deploy your port exceptions and ensure that local administrators do not create less secure settings.

Rationale:

Granting port exceptions could expose the computer to network-based attacks, however not allowing any exceptions is likely to break some applications such as computer management tools

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\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile\Globall
yOpenPorts:AllowUserPrefMerge
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Network\Network Connections\Windows
Firewall\Standard Profile\Windows Firewall: Allow local port exceptions
```

Impact:

If you enable the Windows Firewall: Define inbound port exceptions setting, you can view and change the port exceptions list that is defined by Group Policy. To view and modify the port exceptions list, configure the setting to Enabled and then click the Show button. Note that if you type an invalid definition string, Windows Firewall adds it to the list without checking for errors, which means that you can accidentally create multiple entries for the same port with Scope or Status values that conflict. If you disable the Windows Firewall: Define inbound port exceptions setting, the port exceptions list that is defined by Group Policy is deleted but other settings can continue to open or block ports. Also, if a local port exceptions list exists, it is ignored unless you enable the Windows Firewall: Allow local port exceptions setting. Note If any policy setting opens TCP port 445, Windows Firewall allows inbound ICMP echo request messages (such as those sent by the Ping utility), even if the Windows Firewall: Allow ICMP exceptions policy setting would block them. Policy settings that can open TCP port 445 include Windows Firewall: Allow inbound file and printer sharing exception, Windows Firewall: Allow inbound remote administration exception, and Windows Firewall: Define inbound port exceptions.

1.2.1.1.1.1.18 Configure 'WF_IcmpSettings_AllowInboundEchoRequest' (Not Scored)

Profile Applicability:

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

Description:

If you configure the Windows Firewall: Allow ICMP exceptions setting to Enabled, you must specify which ICMP message types Windows Firewall allows the computer to send or receive.

Rationale:

See parent information.

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\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile\IcmpSet
tings:AllowOutboundParameterProblem
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Network\Network Connections\Windows
Firewall\Standard Profile\WF_IcmpSettings_AllowInboundEchoRequest
```

Impact:

See parent information.

1.2.1.1.1.1.19 Configure 'WF_IcmpSettings_AllowOutboundPacketTooBig' (Not Scored)

Profile Applicability:

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

Description:

If you configure the Windows Firewall: Allow ICMP exceptions setting to Enabled, you must specify which ICMP message types Windows Firewall allows the computer to send or receive.

Rationale:

See parent information.

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\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile\IcmpSet
tings:AllowOutboundParameterProblem
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Network\Network Connections\Windows
Firewall\Standard Profile\WF_IcmpSettings_AllowOutboundPacketTooBig
```

Impact:

See parent information.

1.2.1.1.1.1.20 Configure 'Windows Firewall: Prohibit notifications' (Not Scored)

Profile Applicability:

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

Description:

Windows Firewall can display notifications to users when a program requests that Windows Firewall add the program to the program exceptions list. This situation occurs when programs attempt to open a port and are not allowed to do so because of current Windows Firewall rules. The Windows Firewall: Prohibit notifications setting determines whether these settings are shown to the users. If you configure this policy setting to

Enabled, Windows Firewall prevents the display of these notifications. If you configure it to Disabled, Windows Firewall allows the display of these notifications.

Rationale:

Some organizations may prefer to avoid alarming users when firewall rules block certain types of network activity.

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\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile:Disable
Notifications
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Network\Network Connections\Windows
Firewall\Standard Profile\Windows Firewall: Prohibit notifications
```

Impact:

If you configure this policy setting to Enabled, Windows Firewall prevents the display of these notifications. If you configure it to Disabled, Windows Firewall allows the display of these notifications.

1.2.1.1.1.1.21 Configure 'WF_IcmpSettings_AllowInboundTimestampRequest' (Not Scored)

Profile Applicability:

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

Description:

If you configure the Windows Firewall: Allow ICMP exceptions setting to Enabled, you must specify which ICMP message types Windows Firewall allows the computer to send or receive.

Rationale:

See parent information.

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\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile\IcmpSet
tings:AllowOutboundParameterProblem
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Network\Network Connections\Windows
Firewall\Standard Profile\WF_IcmpSettings_AllowInboundTimestampRequest
```

Impact:

See parent information.

1.2.1.1.1.1.22 Configure 'Windows Firewall: Do not allow exceptions' (Not Scored)

Profile Applicability:

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

Description:

This policy setting caused Windows Firewall to block all unsolicited incoming messages. It overrides all other Windows Firewall settings that allow such messages. If you enable this policy setting in the Windows Firewall item in Control Panel, the Don't allow exceptions check box is selected and administrators cannot clear it.

Rationale:

This policy setting provides a strong defense against external attackers and should be set to Enabled in situations in which you require complete protection from external attacks, such as the outbreak of a new network worm. If you set this policy setting to Disabled, Windows Firewall will be able to apply other policy settings that allow unsolicited incoming messages.

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\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile:DoNotAllowExceptions
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Network\Network Connections\Windows Firewall\Standard Profile\Windows Firewall: Do not allow exceptions
```

Impact:

Many environments contain applications and services that must be allowed to receive inbound unsolicited communications as part of their normal operation. Such environments may need to configure the Windows Firewall: Do not allow exceptions setting to Disabled to allow those applications and services to run properly. However, before you configure this policy setting, you should test the environment to determine exactly what communications need to be allowed.

1.2.1.1.1.1.23 Configure 'Windows Firewall: Protect all network connections' (Not Scored)

Profile Applicability:

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

Description:

This policy setting enables Windows Firewall, which replaces Internet Connection Firewall on all computers that run Windows Vista.

Rationale:

If Windows Firewall: Protect all network connections is configured to Disabled, Windows Firewall is turned off and all other settings for Windows Firewall are ignored. This exposes the computer to potential network-based attacks.

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\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile:EnableF
irewall
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Network\Network Connections\Windows
Firewall\Standard Profile\Windows Firewall: Protect all network connections
```

Impact:

None, this is the default configuration. If you enable this policy setting, Windows Firewall runs and ignores the setting for Computer Configuration\Administrative Templates\Network\Network Connections \Prohibit use of Internet Connection Firewall on your DNS domain network.

1.2.1.1.1.2 Domain Profile

1.2.1.1.1.2.1 Configure 'Windows Firewall: Allow inbound UPnP framework exceptions' (Not Scored)

Profile Applicability:

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

Description:

Microsoft recommends that you avoid the use of this setting, unless required by your environment and your organization's business requirements. This policy setting allows a computer to receive unsolicited Plug and Play messages that are sent by network devices, such as routers with built-in firewalls. To receive these messages, Windows Firewall opens TCP port 2869 and UDP port 1900.

Rationale:

Blocking UPnP network traffic effectively reduces the attack surface of computers in your environment.

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\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\Services\
UPnPFramework:Enabled
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Network\Network Connections\Windows
Firewall\Domain Profile\Windows Firewall: Allow inbound UPnP framework exceptions
```

Impact:

If you enable the Windows Firewall: Allow inbound UPnP framework exceptions setting, Windows Firewall opens these ports so that the computer can receive Plug and Play messages. You must specify the IP addresses or subnets from which these inbound messages are allowed. If you disable this policy setting, Windows Firewall blocks these ports and prevents the computer from receiving Plug and Play messages.

1.2.1.1.1.2.2 Configure 'Windows Firewall: Do not allow exceptions' (Not Scored)

Profile Applicability:

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

Description:

Microsoft recommends that you avoid the use of this setting, unless required by your environment and your organization's business requirements. This policy setting caused Windows Firewall to block all unsolicited incoming messages. It overrides all other Windows Firewall settings that allow such messages. If you enable this policy setting in the Windows Firewall item in Control Panel, the Don't allow exceptions check box is selected and administrators cannot clear it.

Rationale:

This policy setting provides a strong defense against external attackers and should be set to Enabled in situations in which you require complete protection from external attacks, such as the outbreak of a new network worm. If you set this policy setting to Disabled, Windows Firewall will be able to apply other policy settings that allow unsolicited incoming messages.

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\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile:DoNotAllowExceptions
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Network\Network Connections\Windows Firewall\Domain Profile\Windows Firewall: Do not allow exceptions
```

Impact:

Many environments contain applications and services that must be allowed to receive inbound unsolicited communications as part of their normal operation. Such environments may need to configure the Windows Firewall: Do not allow exceptions setting to Disabled to allow those applications and services to run properly. However, before you configure this policy setting, you should test the environment to determine exactly what communications need to be allowed.

1.2.1.1.1.2.3 Configure 'Windows Firewall: Allow local program exceptions' (Not Scored)

Profile Applicability:

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

Description:

This policy setting controls whether administrators can use the Windows Firewall component in Control Panel to define a local program exceptions list.

Rationale:

Granting program exceptions could expose the computer to network-based attacks, however not allowing any exceptions is likely to break some applications such as computer management tools

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\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\Authorize
dApplications:AllowUserPrefMerge
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Network\Network Connections\Windows
Firewall\Domain Profile\Windows Firewall: Allow local program exceptions
```

Impact:

If you disable this policy setting, administrators will not be able to define a local program exceptions list; also, this configuration ensures that program exceptions only come from Group Policy. If this policy setting is enabled, local administrators are allowed to use Control Panel to define program exceptions locally. For enterprise client computers, there may be conditions that justify local program exceptions. These conditions may include applications that were not analyzed when the organization's firewall policy was created or new applications that require nonstandard port configuration. If you choose to enable the Windows Firewall: Allow local program exceptions setting for such situations, remember that the attack surface of the affected computers is increased.

1.2.1.1.1.2.4 Configure 'WF_IcmpSettings_AllowOutboundPacketTooBig' (Not Scored)

Profile Applicability:

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

Description:

Enabled, must specify which ICMP message types Firewall allows the computer to send or receive. Disabled, Firewall blocks all unsolicited inbound ICMP message types and the listed outbound ICMP message types. Utilities that rely on ICMP may fail.

Rationale:

See parent information.

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\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\IcmpSettings:AllowInboundRouterRequest
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Network\Network Connections\Windows Firewall\Domain Profile\WF_IcmpSettings_AllowOutboundPacketTooBig
```

Impact:

See parent information.

1.2.1.1.1.2.5 Configure 'Windows Firewall: Allow local port exceptions' (Not Scored)

Profile Applicability:

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

Description:

The Windows Firewall port exceptions list should be defined by Group Policy, which allows you to centrally manage and deploy your port exceptions and ensure that local administrators do not create less secure settings.

Rationale:

Granting port exceptions could expose the computer to network-based attacks, however not allowing any exceptions is likely to break some applications such as computer management tools

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\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\GloballyO
penPorts:AllowUserPrefMerge
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Network\Network Connections\Windows
Firewall\Domain Profile\Windows Firewall: Allow local port exceptions
```

Impact:

If you enable the Windows Firewall: Define inbound port exceptions setting, you can view and change the port exceptions list that is defined by Group Policy. To view and modify the port exceptions list, configure the setting to Enabled and then click the Show button. Note that if you type an invalid definition string, Windows Firewall adds it to the list without checking for errors, which means that you can accidentally create multiple entries for the same port with Scope or Status values that conflict. If you disable the Windows Firewall: Define inbound port exceptions setting, the port exceptions list that is defined by Group Policy is deleted but other settings can continue to open or block ports. Also, if a local port exceptions list exists, it is ignored unless you enable the Windows Firewall: Allow local port exceptions setting. Note If any policy setting opens TCP port 445, Windows Firewall allows inbound ICMP echo request messages (such as those sent by the Ping utility), even if the Windows Firewall: Allow ICMP exceptions policy setting would block them. Policy settings that can open TCP port 445 include Windows Firewall: Allow inbound file and printer sharing exception, Windows Firewall: Allow inbound remote administration exception, and Windows Firewall: Define inbound port exceptions.

1.2.1.1.1.2.6 Configure 'Windows Firewall: Allow inbound remote administration exception' (Not Scored)

Profile Applicability:

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

Description:

Many organizations take advantage of remote computer administration in their daily operations. To provide flexibility for remote administration, the Windows Firewall: Allow inbound remote administration exception setting is available. If you enable this setting, computers in your environment should accept remote administration requests from as few computers as possible. To maximize the protection provided by Windows Firewall, make sure to specify only the necessary IP addresses and subnets of computers that are used for remote administration.

Rationale:

Some attacks have exploited the ports that are typically used by remote administration programs; Windows Firewall can help block these ports.

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\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\RemoteAdm
inSettings:Enabled
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Network\Network Connections\Windows
Firewall\Domain Profile\Windows Firewall: Allow inbound remote administration
exception
```

Impact:

If this policy setting is enabled, the computer can receive the unsolicited incoming messages that are associated with remote administration on TCP ports 135 and 445. This policy setting also allows Svchost.exe and Lsass.exe to receive unsolicited incoming messages and allows hosted services to open additional dynamically-assigned ports, typically in the range of 1024 to 1034 but potentially anywhere from 1024 to 65535. If you enable this policy setting, you need to specify the IP addresses or subnets from which these incoming messages are allowed. If you configure the Windows Firewall: Allow inbound

remote administration exception setting to Disabled, Windows Firewall makes none of the described exceptions. The impact of configuring this policy setting to Disabled may be unacceptable to many organizations because many remote administration tools and tools that scan for vulnerabilities will fail.

1.2.1.1.1.2.7 Configure 'Windows Firewall: Allow inbound file and printer sharing exception' (Not Scored)

Profile Applicability:

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

Description:

This policy setting creates an exception that allows file and printer sharing. It configures Windows Firewall to open UDP ports 137 and 138 and TCP ports 139 and 445.

Rationale:

Enabling access to file and printer sharing could cause a user to unknowingly expose sensitive data. Additionally, there have been vulnerabilities in the resource sharing features that have been remotely exploitable.

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\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\Services\
FileAndPrint:Enabled
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Network\Network Connections\Windows
Firewall\Domain Profile\Windows Firewall: Allow inbound file and printer sharing
exception
```

Impact:

If you enable this policy setting, Windows Firewall opens these ports so that the computer can receive print jobs and requests for access to shared files. You must specify the IP

addresses or subnets from which such messages are allowed. If you disable the Windows Firewall: Allow inbound file and printer sharing exception setting, Windows Firewall blocks these ports and prevents the computer from sharing files and printers. Note If any policy setting opens TCP port 445, Windows Firewall allows inbound ICMP echo request messages (such as those sent by the Ping utility), even if the Windows Firewall: Allow ICMP exceptions policy setting would block them. Policy settings that can open TCP port 445 include Windows Firewall: Allow inbound file and printer sharing exception, Windows Firewall: Allow inbound remote administration exception, and Windows Firewall: Define inbound port exceptions.

1.2.1.1.1.2.8 Configure 'WF_IcmpSettings_AllowOutboundSourceQuench' (Not Scored)

Profile Applicability:

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

Description:

Enabled, must specify which ICMP message types Firewall allows the computer to send or receive. Disabled, Firewall blocks all unsolicited inbound ICMP message types and the listed outbound ICMP message types. Utilities that rely on ICMP may fail.

Rationale:

See parent information.

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\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\IcmpSetti
ngs:AllowInboundRouterRequest
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Network\Network Connections\Windows
Firewall\Domain Profile\WF_IcmpSettings_AllowOutboundSourceQuench
```

Impact:

See parent information.

1.2.1.1.1.2.9 Configure 'WF_IcmpSettings_AllowOutboundTimeExceeded' (Not Scored)

Profile Applicability:

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

Description:

Enabled, must specify which ICMP message types Firewall allows the computer to send or receive. Disabled, Firewall blocks all unsolicited inbound ICMP message types and the listed outbound ICMP message types. Utilities that rely on ICMP may fail.

Rationale:

See parent information.

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\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\IcmpSetti
ngs:AllowInboundRouterRequest
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Network\Network Connections\Windows
Firewall\Domain Profile\WF_IcmpSettings_AllowOutboundTimeExceeded
```

Impact:

See parent information.

1.2.1.1.1.2.10 Configure 'Windows Firewall: Allow ICMP exceptions' (Not Scored)

Profile Applicability:

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

Description:

This policy setting defines the set of Internet Control Message Protocol (ICMP) message types that Windows Firewall allows. Utilities can use ICMP messages to determine the status of other computers. For example, Ping uses the echo request message. If you configure the Windows Firewall: Allow ICMP exceptions setting to Enabled, you must specify which ICMP message types Windows Firewall allows the computer to send or receive. When you configure this policy setting to Disabled, Windows Firewall blocks all unsolicited inbound ICMP message types and the listed outbound ICMP message types. As a result, utilities that rely on ICMP may fail. Many attacker tools take advantage of computers that accept ICMP message types and use these messages to mount a variety of attacks. However, some applications require some ICMP messages in order to function properly. Also, ICMP messages are used to estimate network performance when Group Policy is downloaded and processed; if ICMP messages are blocked, Group Policy may not be applied to affected systems. For that reason, it is recommended that you configure the Windows Firewall: Allow ICMP exceptions setting to Disabled whenever possible. If your environment requires some ICMP messages to get through Windows Firewall, configure this policy setting with the appropriate message types. Whenever the computer is on an untrusted network, the Windows Firewall: Allow ICMP exceptions setting should be configured to Disabled. Note If any policy setting opens TCP port 445, Windows Firewall allows inbound ICMP echo request messages (such as those sent by the Ping utility), even if the Windows Firewall: Allow ICMP exceptions policy setting would block them. Policy settings that can open TCP port 445 include Windows Firewall: Allow inbound file and printer sharing exception, Windows Firewall: Allow inbound remote administration exception, and Windows Firewall: Define inbound port exceptions.

Rationale:

Many attacker tools take advantage of computers that accept ICMP message types and use these messages to mount a variety of attacks.

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\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\IcmpSetti
ngs:AllowInboundRouterRequest
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Network\Network Connections\Windows
Firewall\Domain Profile\Windows Firewall: Allow ICMP exceptions
```

Impact:

If you configure the Windows Firewall: Allow ICMP exceptions setting to Enabled, you must specify which ICMP message types Windows Firewall allows the computer to send or receive. When you configure this policy setting to Disabled, Windows Firewall blocks all unsolicited inbound ICMP message types and the listed outbound ICMP message types. As a result, utilities that rely on ICMP may fail. Some applications require some ICMP messages in order to function properly. Also, ICMP messages are used to estimate network performance when Group Policy is downloaded and processed; if ICMP messages are blocked, Group Policy may not be applied to affected systems. Note If any policy setting opens TCP port 445, Windows Firewall allows inbound ICMP echo request messages (such as those sent by the Ping utility), even if the Windows Firewall: Allow ICMP exceptions policy setting would block them. Policy settings that can open TCP port 445 include Windows Firewall: Allow inbound file and printer sharing exception, Windows Firewall: Allow inbound remote administration exception, and Windows Firewall: Define inbound port exceptions.

1.2.1.1.1.2.11 Configure 'WF_IcmpSettings_AllowOutboundParameterProblem' (Not Scored)

Profile Applicability:

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

Description:

Enabled, must specify which ICMP message types Firewall allows the computer to send or receive. Disabled, Firewall blocks all unsolicited inbound ICMP message types and the listed outbound ICMP message types. Utilities that rely on ICMP may fail.

Rationale:

See parent information.

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\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\IcmpSettings:AllowInboundRouterRequest
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Network\Network Connections\Windows Firewall\Domain Profile\WF_IcmpSettings_AllowOutboundParameterProblem
```

Impact:

See parent information.

1.2.1.1.1.2.12 Configure 'WF_IcmpSettings_AllowInboundEchoRequest' (Not Scored)

Profile Applicability:

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

Description:

Enabled, must specify which ICMP message types Firewall allows the computer to send or receive. Disabled, Firewall blocks all unsolicited inbound ICMP message types and the listed outbound ICMP message types. Utilities that rely on ICMP may fail.

Rationale:

See parent information.

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\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\IcmpSetti
ngs:AllowInboundRouterRequest
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Network\Network Connections\Windows
Firewall\Domain Profile\WF_IcmpSettings_AllowInboundEchoRequest
```

Impact:

See parent information.

1.2.1.1.1.2.13 Configure 'WF_IcmpSettings_AllowInboundMaskRequest' (Not Scored)

Profile Applicability:

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

Description:

Enabled, must specify which ICMP message types Firewall allows the computer to send or receive. Disabled, Firewall blocks all unsolicited inbound ICMP message types and the listed outbound ICMP message types. Utilities that rely on ICMP may fail.

Rationale:

See parent information.

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\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\IcmpSettings:AllowInboundRouterRequest
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Network\Network Connections\Windows Firewall\Domain Profile\WF_IcmpSettings_AllowInboundMaskRequest
```

Impact:

See parent information.

1.2.1.1.1.2.14 Configure 'WF_IcmpSettings_AllowRedirect' (Not Scored)

Profile Applicability:

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

Description:

Enabled, must specify which ICMP message types Firewall allows the computer to send or receive. Disabled, Firewall blocks all unsolicited inbound ICMP message types and the listed outbound ICMP message types. Utilities that rely on ICMP may fail.

Rationale:

See parent information.

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\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\IcmpSettings:AllowInboundRouterRequest
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Network\Network Connections\Windows
Firewall\Domain Profile\WF_IcmpSettings_AllowRedirect
```

Impact:

See parent information.

1.2.1.1.1.2.15 Configure 'Windows Firewall: Prohibit notifications' (Not Scored)

Profile Applicability:

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

Description:

Unless required by your environment and your organization's business requirements you may wish to avoid using this setting because the notifications can help users to understand why certain applications aren't working as expected. Windows Firewall can display notifications to users when a program requests that Windows Firewall add the program to the program exceptions list. This situation occurs when programs attempt to open a port and are not allowed to do so because of current Windows Firewall rules. The Windows Firewall: Prohibit notifications setting determines whether these settings are shown to the users.

Rationale:

Some organizations may prefer to avoid alarming users when firewall rules block certain types of network activity.

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\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile:DisableNo
tifications
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Network\Network Connections\Windows
Firewall\Domain Profile\Windows Firewall: Prohibit notifications
```

Impact:

If you configure this policy setting to Enabled, Windows Firewall prevents the display of these notifications. If you configure it to Disabled, Windows Firewall allows the display of these notifications.

1.2.1.1.1.2.16 Configure 'Windows Firewall: Define inbound port exceptions' (Not Scored)

Profile Applicability:

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

Description:

Microsoft recommends that you avoid the use of this setting, unless required by your environment and your organization's business requirements; specifying allowed applications using the Define inbound program exceptions is usually a more secure approach. The Windows Firewall port exceptions list should be defined by Group Policy, which allows you to centrally manage and deploy your port exceptions and ensure that local administrators do not create less secure settings.

Rationale:

Granting port exceptions could expose the computer to network-based attacks, however not allowing any exceptions is likely to break some applications such as computer management tools

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\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\GloballyO
penPorts:Enabled
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Network\Network Connections\Windows
Firewall\Domain Profile\Windows Firewall: Define inbound port exceptions
```

Impact:

If you enable the Windows Firewall: Define inbound port exceptions setting, you can view and change the port exceptions list that is defined by Group Policy. To view and modify the port exceptions list, configure the setting to Enabled and then click the Show button. Note that if you type an invalid definition string, Windows Firewall adds it to the list without checking for errors, which means that you can accidentally create multiple entries for the same port with Scope or Status values that conflict. If you disable the Windows Firewall: Define inbound port exceptions setting, the port exceptions list that is defined by Group Policy is deleted but other settings can continue to open or block ports. Also, if a local port exceptions list exists, it is ignored unless you enable the Windows Firewall: Allow local port exceptions setting. Note If any policy setting opens TCP port 445, Windows Firewall allows inbound ICMP echo request messages (such as those sent by the Ping utility), even if the Windows Firewall: Allow ICMP exceptions policy setting would block them. Policy settings that can open TCP port 445 include Windows Firewall: Allow inbound file and printer sharing exception, Windows Firewall: Allow inbound remote administration exception, and Windows Firewall: Define inbound port exceptions.

1.2.1.1.1.2.17 Configure 'WF_IcmpSettings_AllowInboundRouterRequest' (Not Scored)

Profile Applicability:

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

Description:

Enabled, must specify which ICMP message types Firewall allows the computer to send or receive. Disabled, Firewall blocks all unsolicited inbound ICMP message types and the listed outbound ICMP message types. Utilities that rely on ICMP may fail.

Rationale:

See parent information.

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\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\IcmpSettings:AllowInboundRouterRequest
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Network\Network Connections\Windows Firewall\Domain Profile\WF_IcmpSettings_AllowInboundRouterRequest
```

Impact:

See parent information.

1.2.1.1.1.2.18 Configure 'WF_IcmpSettings_AllowOutboundDestinationUnreachable' (Not Scored)

Profile Applicability:

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

Description:

Enabled, must specify which ICMP message types Firewall allows the computer to send or receive. Disabled, Firewall blocks all unsolicited inbound ICMP message types and the listed outbound ICMP message types. Utilities that rely on ICMP may fail.

Rationale:

See parent information.

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\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\IcmpSettings:AllowInboundRouterRequest
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Network\Network Connections\Windows
Firewall\Domain Profile\WF_IcmpSettings_AllowOutboundDestinationUnreachable
```

Impact:

See parent information.

1.2.1.1.1.2.19 Configure 'Windows Firewall: Protect all network connections' (Not Scored)

Profile Applicability:

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

Description:

This policy setting enables Windows Firewall, which replaces Internet Connection Firewall on all computers that run Windows Vista.

Rationale:

If Windows Firewall: Protect all network connections is configured to Disabled, Windows Firewall is turned off and all other settings for Windows Firewall are ignored. This exposes the computer to potential network-based attacks.

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\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile:EnableFir
ewall
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Network\Network Connections\Windows
Firewall\Domain Profile\Windows Firewall: Protect all network connections
```

Impact:

None, this is the default configuration. If you enable this policy setting, Windows Firewall runs and ignores the setting for Computer Configuration\Administrative Templates\Network\Network Connections \Prohibit use of Internet Connection Firewall on your DNS domain network.

1.2.1.1.1.2.20 Configure 'Windows Firewall: Prohibit unicast response to multicast or broadcast requests' (Not Scored)

Profile Applicability:

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

Description:

This policy setting helps prevent a computer from receiving unicast responses to its outgoing multicast or broadcast messages.

Rationale:

Typically, you would not want to receive unicast responses to multicast or broadcast messages. Such responses can indicate a denial of service (DoS) attack or an attempt to probe a known computer.

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\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile:DisableUnicastResponsesToMulticastBroadcast
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Network\Network Connections\Windows Firewall\Domain Profile\Windows Firewall: Prohibit unicast response to multicast or broadcast requests
```

Impact:

Note This policy setting has no effect if the unicast message is a response to a DHCP broadcast message that is sent by the computer. Windows Firewall always permits those

DHCP responses. However, this policy setting can interfere with the NetBIOS messages that detect name conflicts.

1.2.1.1.1.2.21 Configure 'Windows Firewall: Define inbound program exceptions' (Not Scored)

Profile Applicability:

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

Description:

Some applications may need to open and use network ports that are not typically allowed by Windows Firewall. The Windows Firewall: Define inbound program exceptions setting allows you to view and change the program exceptions list that is defined by Group Policy.

Rationale:

There is risk that inbound exceptions will be made to programs that have software vulnerabilities, however, if exceptions are not allowed then management programs and other useful applications will fail.

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\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\Authorize
dApplications:Enabled
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Network\Network Connections\Windows
Firewall\Domain Profile\Windows Firewall: Define inbound program exceptions
```

Impact:

If this policy setting is Enabled you can view and change the program exceptions list. If you add a program to this list and set its status to Enabled, that program can receive unsolicited incoming messages on any port that it requests Windows Firewall to open, even if that port

is blocked by another setting. If you configure this policy setting to Disabled, the program exceptions list that is defined by Group Policy is deleted. Note If you type an invalid definition string, Windows Firewall adds it to the list without checking for errors. Because the entry is not checked, you can add programs that you have not installed yet. You can also accidentally create multiple exceptions for the same program with Scope or Status values that conflict.

1.2.1.1.1.2.22 Configure 'WF_IcmpSettings_AllowInboundTimestampRequest' (Not Scored)

Profile Applicability:

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

Description:

Enabled, must specify which ICMP message types Firewall allows the computer to send or receive. Disabled, Firewall blocks all unsolicited inbound ICMP message types and the listed outbound ICMP message types. Utilities that rely on ICMP may fail.

Rationale:

See parent information.

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\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\IcmpSetti
ngs:AllowInboundRouterRequest
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Network\Network Connections\Windows
Firewall\Domain Profile\WF_IcmpSettings_AllowInboundTimestampRequest
```

Impact:

See parent information.

1.2.1.1.1.2.23 Configure 'Windows Firewall: Allow inbound Remote Desktop exceptions' (Not Scored)

Profile Applicability:

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

Description:

Many organizations use Remote Desktop connections in their normal troubleshooting procedures or operations. To provide flexibility for remote administration, the Windows Firewall: Allow inbound Remote Desktop exceptions setting is available.

Rationale:

Some attacks have exploited the ports that are typically used by Remote Desktop.

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\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\Services\
RemoteDesktop:Enabled
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Network\Network Connections\Windows
Firewall\Domain Profile\Windows Firewall: Allow inbound Remote Desktop exceptions
```

Impact:

If you enable this policy setting, Windows Firewall opens TCP port 3389 for inbound connections. You must also specify the IP addresses or subnets from which these inbound messages are allowed. If you disable this policy setting, Windows Firewall blocks this port and prevents the computer from receiving Remote Desktop requests. If an administrator adds this port to a local port exceptions list in an attempt to open it, Windows Firewall does not open the port. Computers in your environment should accept Remote Desktop requests from as few computers as possible.

1.2.2 System

1.2.2.1 Remote Assistance

1.2.2.1.1 Configure 'RA_Solicit_ExpireUnits_List' (Not Scored)

Profile Applicability:

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

Description:

If the Solicited Remote Assistance setting is enabled, the following options are available: . Allow helpers to remotely control the computer . Allow helpers to only view the computer

Rationale:

See parent information.

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\Software\policies\Microsoft\Windows NT\Terminal
Services:fAllowToGetHelp
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\System\Remote
Assistance\RA_Solicit_ExpireUnits_List
```

Impact:

See parent information.

1.2.2.1.2 Configure 'RA_Solicit_Control_List' (Not Scored)

Profile Applicability:

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

Description:

If the Solicited Remote Assistance setting is enabled, the following options are available: . Allow helpers to remotely control the computer . Allow helpers to only view the computer

Rationale:

See parent information.

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\Software\policies\Microsoft\Windows NT\Terminal
Services:fAllowToGetHelp
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\System\Remote
Assistance\RA_Solicit_Control_List
```

Impact:

See parent information.

1.2.2.1.3 Configure 'Offer Remote Assistance' (Not Scored)

Profile Applicability:

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

Description:

This policy setting determines whether a support person or an IT expert administrator can offer remote assistance to computers in your environment if a user does not explicitly request assistance first through a channel, such as e-mail, or Instant Messenger. Note The expert cannot connect to the computer unannounced or control it without permission from

the user. When the 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 after the Offer Remote Assistance setting is configured to Enabled. If this policy setting is enabled the following options are available: . Allow helpers to only view the computer . Allow helpers to remotely control the computer When you configure this policy setting, you can also specify a list of users or user groups known as helpers who may offer remote assistance. To configure the list of helpers 1. In the Offer Remote Assistance setting configuration window, click Show. A new window will open in which you can enter helper names. 2. Add each user or group to the Helper list in one of the following formats: . <Domain Name>\<User Name> . <Domain Name>\<Group Name> If this policy setting is disabled or not configured, users and or groups will not be able to offer unsolicited remote assistance to computer users in your environment.

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 for your organization. This group policy object is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\policies\Microsoft\Windows NT\Terminal
Services:fAllowUnsolicited
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\System\Remote Assistance\Offer Remote
Assistance
```

Impact:

Help desk and support personnel will not be able to proactively offer assistance, although they can still respond to user assistance requests.

1.2.2.1.4 Configure 'RA_Solicit_ExpireValue_Edt' (Not Scored)

Profile Applicability:

- Level 1 - Domain Controller

- Level 1 - Member Server

Description:

If the Solicited Remote Assistance setting is enabled, the following options are available: . Allow helpers to remotely control the computer . Allow helpers to only view the computer

Rationale:

See parent information.

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\Software\policies\Microsoft\Windows NT\Terminal
Services:fAllowToGetHelp
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\System\Remote
Assistance\RA_Solicit_ExpireValue_Edt
```

Impact:

See parent information.

1.2.2.1.5 Configure 'RA_Solicit_Mailto_List' (Not Scored)

Profile Applicability:

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

Description:

If the Solicited Remote Assistance setting is enabled, the following options are available: . Allow helpers to remotely control the computer . Allow helpers to only view the computer

Rationale:

See parent information.

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\Software\policies\Microsoft\Windows NT\Terminal
Services:fAllowToGetHelp
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\System\Remote
Assistance\RA_Solicit_Mailto_List
```

Impact:

See parent information.

1.2.2.1.6 Configure 'Solicited Remote Assistance' (Not Scored)

Profile Applicability:

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

Description:

This policy setting determines whether remote assistance may be solicited from computers running Windows operating systems in your environment. You can enable this policy setting to allow users to solicit remote assistance from IT expert administrators. If the Solicited Remote Assistance setting is enabled, the following options are available: . Allow helpers to remotely control the computer . Allow helpers to only view the computer Also, the following options are available to configure the amount of time that a user help request remains valid: . Maximum ticket time (value): . Maximum ticket time (units): hours, minutes or days When a ticket (help request) expires, the user must send another request before an expert can connect to the computer. If you disable the Solicited Remote Assistance setting, users cannot send help requests and the expert cannot connect to their computers. If the Solicited Remote Assistance setting is not configured, users can configure solicited remote assistance through the Control Panel. The following settings are enabled by default in the Control Panel: Solicited Remote Assistance, Buddy support, and Remote control. The value for the Maximum ticket time is set to 30 days. If this policy setting is disabled, no one will be able to access Windows Vista client computers across the network.

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 for your organization. This group policy object is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\policies\Microsoft\Windows NT\Terminal
Services:fAllowToGetHelp
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\System\Remote Assistance\Solicited
Remote Assistance
```

Impact:

If you enable this policy, users on this computer can use e-mail or file transfer to ask someone for help. Also, users can use instant messaging programs to allow connections to this computer, and you can configure additional Remote Assistance settings. If you disable this policy, 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. If you don't configure this policy, users can enable or disable Solicited (Ask for) Remote Assistance themselves in System Properties in Control Panel. Users can also configure Remote Assistance settings. If you enable this policy setting, you have two ways to allow helpers to provide Remote Assistance: "Allow helpers to only view the computer" or "Allow helpers to remotely control the computer." The "Maximum ticket time" setting sets a limit on the amount of time that a Remote Assistance invitation created by using e-mail or file transfer can remain open. The "Select the method for sending e-mail invitations" setting specifies which e-mail standard to use to send Remote Assistance invitations. Depending on your e-mail program, you can use either the Mailto standard (the invitation recipient connects through an Internet link) or the SMAPI (Simple MAPI) standard (the invitation is attached to your e-mail message). This setting is not available in Windows Vista since SMAPI is the only method supported. If you enable this policy you

should also enable appropriate firewall exceptions to allow Remote Assistance communications.

1.2.2.2 Internet Communication Management

1.2.2.2.1 Internet Communication settings

1.2.2.2.1.1 Configure 'Turn off Windows Update device driver searching' (Not Scored)

Profile Applicability:

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

Description:

This policy setting specifies whether Windows will search Windows Update for device drivers when no local drivers for a device are present. Note See also Turn off Windows Update device driver search prompt in Administrative Templates/System, which governs whether an administrator is prompted before Windows Update is searched for device drivers if a driver is not found locally.

Rationale:

If users are able to download and install device drivers there is a small chance that they will install a driver that reduces system stability. There is an even smaller possibility that they will install a driver that includes malicious code. These risks are very low because Microsoft requires vendors to test drivers extensively before they can be published on Windows Update.

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\Software\Policies\Microsoft\Windows\DriverSearching:DontSearchWindo
wsUpdate
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\System\Internet Communication
Management\Internet Communication settings\Turn off Windows Update device driver
searching
```

Impact:

Users will not be able to download new or updated device drivers from Windows Update.

1.2.2.2.1.2 Configure 'Turn off Search Companion content file updates' (Not Scored)

Profile Applicability:

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

Description:

This policy setting specifies whether Search Companion should automatically download content updates during local and Internet searches.

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 for your organization. This group policy object is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\SearchCompanion:DisableContentFileUpdat
es
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

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

Impact:

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.

1.2.2.2.1.3 Configure 'Turn off Internet download for Web publishing and online ordering wizards' (Not 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.

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 for your organization. This group policy object is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer:NoWebSe
rvices
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

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

Impact:

If this policy setting is enabled, Windows is prevented from downloading providers; only the service providers cached in the local registry will display.

1.2.2.2.1.4 Configure 'Turn off the Windows Messenger Customer Experience Improvement Program' (Not Scored)

Profile Applicability:

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

Description:

This policy setting specifies whether Windows Messenger can collect anonymous information about how the Windows Messenger software and service is used.

Rationale:

Large enterprise environments may not want to have information collected from managed client computers.

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\Software\Policies\Microsoft\Messenger\Client:CEIP
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

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

Impact:

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.

1.2.2.2.1.5 Configure 'Turn off printing over HTTP' (Not Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

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 environments.

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\Software\Policies\Microsoft\Windows NT\Printers:DisableHTTPPrinting
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

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

Impact:

If you enable this policy setting, the client computer will not be able to print to Internet printers over HTTP. 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.

1.2.2.2.1.6 Configure 'Turn off the "Publish to Web" task for files and folders' (Not Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - 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.

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 for your organization. This group policy object is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer:NoPublishingWizard
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

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

Impact:

The Web Publishing wizard is used to download a list of providers and allow users to publish content to the Web.

1.2.2.2.1.7 Configure 'Turn off downloading of print drivers over HTTP' (Not 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.

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 for your organization. This group policy object is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows
NT\Printers:DisableWebPnPDownload
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

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

Impact:

This policy setting does not prevent the client computer from printing to printers on the intranet or the Internet over HTTP. It only prohibits drivers that are not already installed locally from downloading.

1.2.2.3 Group Policy

1.2.2.3.1 Configure 'Registry policy processing' (Not Scored)

Profile Applicability:

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

Description:

This policy setting determines when registry policies are updated. It affects all policies in the Administrative Templates folder, and any other policies that store values in the

registry. If this policy setting is enabled, the following options are available: . Do not apply during periodic background processing. . Process even if the Group Policy objects have not changed. Some settings that are configured through the Administrative Templates are made in areas of the registry that are accessible to users. User changes to these settings will be overwritten if this policy setting is enabled.

Rationale:

You can enable this setting and then select the Process even if the Group Policy objects have not changed option to ensure that the policies will be reprocessed even if none have been changed. This way, any 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 for your organization. This group policy object is backed by the following registry location:

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

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\System\Group Policy\Registry policy processing
```

Impact:

Group Policies will be reapplied every time they are refreshed, which could have a slight impact on performance.

1.2.2.3.2 Configure 'CSE_NOBACKGROUND10' (Not Scored)

Profile Applicability:

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

Description:

If this policy setting is enabled, the following options are available: . Do not apply during periodic background processing. . Process even if the Group Policy objects have not changed.

Rationale:

See parent information.

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

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\System\Group Policy\CSE_NOBACKGROUND10
```

Impact:

See parent information.

1.2.2.3.3 Configure 'CSE_NOCHANGES10' (Not Scored)

Profile Applicability:

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

Description:

If this policy setting is enabled, the following options are available: . Do not apply during periodic background processing. . Process even if the Group Policy objects have not changed.

Rationale:

See parent information.

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

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\System\Group Policy\CSE_NOCHANGES10
```

Impact:

See parent information.

1.2.2.4 Remote Procedure Call

1.2.2.4.1 Configure 'RPC Endpoint Mapper Client Authentication' (Not Scored)

Profile Applicability:

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

Description:

If you enable this policy setting, client computers that communicate with this computer are forced to provide authentication before RPC communication can be established. By default, RPC clients do not use authentication to communicate with the RPC Server Endpoint Mapper Service when they request the endpoint of a server.

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 for your organization. This group policy object is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\Rpc:EnableAuthEpResolution
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\System\Remote Procedure Call\RPC
Endpoint Mapper Client Authentication
```

Impact:

RPC clients will be forced to authenticate before they can begin communicating with the desired RPC service, this means that anonymous access will not be available and RPC clients that do not support authentication will fail.

1.2.2.4.2 Configure 'Restrictions for Unauthenticated RPC clients' (Not Scored)

Profile Applicability:

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

Description:

This policy setting configures the RPC Runtime on an RPC server to restrict unauthenticated RPC clients from connecting to the RPC server. 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 asked to be accessible by unauthenticated clients may be exempt from this restriction, depending on the selected value for this policy.

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 for your organization. This group policy object is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\Rpc:RestrictRemoteClients
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\System\Remote Procedure
Call\Restrictions for Unauthenticated RPC clients
```

Impact:

RPC applications that do not authenticate unsolicited inbound connection requests may not work properly when this configuration is applied. Ensure you test applications before you deploy this policy setting throughout your environment. Although the Authenticated value for this policy setting is not completely secure, it can be useful for providing application compatibility in your environment.

1.2.2.5 Logon

1.2.2.5.1 Configure 'Do not process the legacy run list' (Not Scored)

Profile Applicability:

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

Description:

This policy setting causes the run list, which is a list of programs that Windows runs automatically when it starts, to be ignored. The customized run lists for Windows Vista are stored in the registry at the following locations: . HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run . HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run You can enable the Do not process the legacy run list setting to help prevent a malicious user from running a program each time Windows Vista starts, which could compromise data on the computer or cause other harm. When this policy setting is enabled, certain system programs are prevented from running, such as antivirus software, and software distribution and monitoring software. It is recommended to evaluate the threat level to

your environment before you determine whether to use this policy setting for your organization.

Rationale:

A malicious user could configure a program to be run each time Windows starts that could compromise data on the computer or cause other harm.

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\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer:Disable
LocalMachineRun
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\System\Logon\Do not process the legacy
run list
```

Impact:

If you enable this setting, certain computer programs such as antivirus software and software distribution and monitoring software are also prevented from execution. You should evaluate the threat level to your environment that this setting is designed to safeguard against before you decide on a strategy to use this setting for your organization.

1.2.2.5.2 Configure 'Do not process the run once list' (Not Scored)

Profile Applicability:

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

Description:

This policy setting causes the run once list, which is the list of programs that Windows Vista runs automatically when it starts, to be ignored. This policy setting differs from the Do not process the legacy run list setting in that programs on this list will run once the next time the client computer restarts and an administrator logs on. Setup and installation programs are sometimes added to this list to complete installations after a client computer

restarts. If you enable this policy setting, attackers generally cannot use the run once list to launch rogue applications, which was a common method of attack in the past. A malicious user can exploit the run once list to install a program that may compromise the security of Windows Vista based client computers, however since editing this list requires administrator privileges the importance of configuring this setting is not high.

Rationale:

A malicious user can exploit the run once list to install a program that may compromise the security of Windows clients.

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\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer:Disable
LocalMachineRunOnce
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\System\Logon\Do not process the run
once list
```

Impact:

If you enable the Do not process the run once list setting you should experience minimal functionality loss for users in your environment, especially if the clients have been configured with all of your organization's standard software before you apply this setting through Group Policy. However, this configuration may prevent some setup and installation programs, such as Internet Explorer, from working properly.

1.2.3 Windows Components

1.2.3.1 AutoPlay Policies

1.2.3.1.1 Set 'Turn off Autoplay' 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. You can enable the Turn off Autoplay setting to disable the Autoplay feature. 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.

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 object is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer:NoDrive
TypeAutoRun
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`. Then set the available option to `All drives`.

```
Computer Configuration\Administrative Templates\Windows Components\AutoPlay
Policies\Turn off Autoplay
```

Impact:

Users will have to manually launch setup or installation programs that are provided on removable media.

1.2.3.2 Windows Update

1.2.3.2.1 Configure 'AutoUpdateSchDay' (Not Scored)

Profile Applicability:

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

Description:

Enabled, the OS recognizes a network connection available and searches Windows Update or designated intranet site for updates that apply (additonal settings required). Disabled you will need to download and manually install available updates.

Rationale:

See parent information.

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\Software\Policies\Microsoft\Windows\WindowsUpdate\AU:NoAutoUpdate
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Windows Components\Windows
Update\AutoUpdateSchDay
```

Impact:

See parent information.

1.2.3.2.2 Configure 'Specify intranet Microsoft update service location' (Not Scored)

Profile Applicability:

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

Description:

This policy setting allows you to specify an intranet server to host updates from the Microsoft Update Web site. You can then use this update service location to automatically update computers on your network. The Automatic Updates client will search this service for updates that apply to the computers on your network. To use the Specify intranet Microsoft update service location setting, you must set two server name values: the server from which the Automatic Updates client detects and downloads updates, and the server to which updated workstations upload statistics. You can set both values to be the same server. If you enable the Specify intranet Microsoft update service location setting, the Automatic Updates client will connect to the specified intranet Microsoft update service server (instead of Windows Update) to search for and download updates. This configuration allows end users in your organization to avoid firewall issues, and provides you with an opportunity to test updates before you deploy them. If you disable or do not configure this policy setting, the Automatic Updates client will connect directly to the Windows Update site on the Internet (if Automatic Updates is not disabled by Group Policy or user preference).

Rationale:

By default, Automatic Updates will attempt to download updates from the Microsoft Windows Update Web site. Some organizations want to verify that all new updates are compatible with their particular environment before they are deployed. Also, if you configure an internal Software Update Services (SUS) server you will help reduce the load on perimeter firewalls, routers, and proxy servers, as well as the load on external network links.

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\Software\Policies\Microsoft\Windows\WindowsUpdate:WUServer
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Windows Components\Windows
Update\Specify intranet Microsoft update service location
```

Impact:

Critical updates and service packs will have to be proactively managed by the organization's IT staff.

1.2.3.2.3 Configure 'No auto-restart with logged on users for scheduled automatic updates installations' (Not 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. If you enable the No auto-restart for scheduled Automatic Updates installations setting, Automatic Updates does not restart computers automatically during scheduled installations. Instead, Automatic Updates notifies users to restart their computers to complete the installations. You should note that Automatic Updates will not be able to detect future updates until restarts occur on the affected computers. If you disable or do not configure this setting, Automatic Updates will notify users that their computers will automatically restart in 5 minutes to complete the installations. The possible values for the No auto-restart for scheduled Automatic Updates installations setting are: . Enabled . Disabled . Not Configured 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:

Sometimes updates require updated computers to 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.

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\Software\Policies\Microsoft\Windows\WindowsUpdate\AU:NoAutoRebootWithLoggedOnUsers
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Windows Components\Windows Update\No auto-restart with logged on users for scheduled automatic updates installations
```

Impact:

If you enable this policy setting, the operating systems on the servers in your environment will restart themselves automatically. For critical servers this could lead to temporary but unexpected, DoS conditions.

1.2.3.2.4 Configure 'CorpWUURL' (Not Scored)

Profile Applicability:

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

Description:

This policy setting allows you to specify an intranet server to host updates from the Microsoft Update Web site.

Rationale:

See parent information.

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\Software\Policies\Microsoft\Windows\WindowsUpdate:WUServer
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Windows Components\Windows Update\CorpWUURL_Name
```

Impact:

See parent information.

1.2.3.2.5 Configure 'Configure Automatic Updates' (Not 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: . Notify before downloading any updates and notify again before installing them. . Download the updates automatically and notify when they are ready to be installed. (Default setting) . Automatically download updates and install them on the schedule specified below. If you disable this policy setting, you will need to download and manually install any available updates from Windows Update.

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 for your organization. This group policy object is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate\AU:NoAutoUpdate
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Windows Components\Windows
Update\Configure Automatic Updates
```

Impact:

Critical operating system updates and service packs will automatically download and install at 3:00 A.M. daily.

1.2.3.2.6 Configure 'Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box' (Not Scored)

Profile Applicability:

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

Description:

This policy setting allows you to manage whether the Install Updates and Shut Down option is displayed in the Shut Down Windows dialog box. This policy setting works in conjunction with the following Do not adjust default option to ˜Install Updates and Shut Down' in Shut Down Windows Dialog box setting.

Rationale:

Updates are important for maintaining the ongoing security of a computer, therefore this setting should not be enabled.

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\Software\Policies\Microsoft\Windows\WindowsUpdate\AU:NoAUShutdownOp
tion
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Windows Components\Windows Update\Do
not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box
```

Impact:

If you disable this policy setting, the Install Updates and Shut Down option will display in the Shut Down Windows dialog box if updates are available when the user selects the Shut Down option in the Start menu.

1.2.3.2.7 Configure 'AutoUpdateSchTime' (Not Scored)

Profile Applicability:

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

Description:

Enabled, the OS recognizes a network connection available and searches Windows Update or designated intranet site for updates that apply (additonal settings required). Disabled you will need to download and manually install available updates.

Rationale:

See parent information.

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\Software\Policies\Microsoft\Windows\WindowsUpdate\AU:NoAutoUpdate
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Windows Components\Windows
Update\AutoUpdateSchTime
```

Impact:

See parent information.

1.2.3.2.8 Configure 'Do not adjust default option to 'Install Updates and Shut Down' in Shut Down Windows dialog box' (Not Scored)

Profile Applicability:

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

Description:

This policy setting allows you to manage whether the 'Install Updates and Shut Down' option is allowed to be the default choice in the Shut Down Windows dialog. Note that this policy setting has no impact if the Computer Configuration\Administrative Templates\Windows Components\Windows Update\Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box policy setting is enabled.

Rationale:

Updates are important for maintaining the ongoing security of a computer, therefore this setting should not be enabled.

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\Software\Policies\Microsoft\Windows\WindowsUpdate\AU:NoAUAsDefaultShutdownOption
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Windows Components\Windows Update\Do not adjust default option to 'Install Updates and Shut Down' in Shut Down Windows dialog box
```

Impact:

If you enable this policy setting, the user's last shut down choice (Hibernate, Restart, etc.) is the default option in the Shut Down Windows dialog box, regardless of whether the 'Install Updates and Shut Down' option is available in the 'What do you want the computer to do?' list. If you disable or do not configure this policy setting, the 'Install Updates and Shut Down' option will be the default option in the Shut Down Windows dialog box if updates are available for installation at the time the user selects the Shut Down option in the Start menu.

1.2.3.2.9 Configure 'Reschedule Automatic Updates scheduled installations' (Not Scored)

Profile Applicability:

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

Description:

This policy setting determines the amount of time before previously scheduled Automatic Update installations will proceed after system startup. If you configure this policy setting to Enabled, a previously scheduled installation will begin after a specified number of minutes when you next start the computer. If you configure this policy setting to Disabled or Not configured, previously scheduled installations will occur during the next regularly scheduled installation time. Note: This policy setting only works when Automatic Updates is configured to perform scheduled update installations. If the Configure Automatic Updates setting is Disabled, the Reschedule Automatic Updates scheduled installations setting has no effect. You can enable the latter two settings to ensure that previously missed installations will be scheduled to install each time the computer restarts.

Rationale:

If Automatic Updates is not forced to wait a few minutes after a restart, computers in your environment might not have enough time to completely start all of their applications and services. If you specify enough time after a restart, new update installations should not conflict with the computer's startup procedures.

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\Software\Policies\Microsoft\Windows\WindowsUpdate\AU:RescheduleWaitTimeEnabled
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Windows Components\Windows Update\Reschedule Automatic Updates scheduled installations
```

Impact:

Automatic Updates will not start until 10 minutes after the computer restarts.

1.2.3.2.10 Configure 'CorpWUStatusURL' (Not Scored)

Profile Applicability:

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

Description:

This policy setting allows you to specify an intranet server to host updates from the Microsoft Update Web site.

Rationale:

See parent information.

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\Software\Policies\Microsoft\Windows\WindowsUpdate:WUServer
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Windows Components\Windows
Update\CorpWUStatusURL_Name
```

Impact:

See parent information.

1.2.3.2.11 Configure 'AutoUpdateMode' (Not Scored)

Profile Applicability:

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

Description:

Enabled, the OS recognizes a network connection available and searches Windows Update or designated intranet site for updates that apply (additonal settings required). Disabled you will need to download and manually install available updates.

Rationale:

See parent information.

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\Software\Policies\Microsoft\Windows\WindowsUpdate\AU:NoAutoUpdate
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Windows Components\Windows
Update\AutoUpdateMode
```

Impact:

See parent information.

1.2.3.3 Windows Messenger

1.2.3.3.1 Configure 'Do not allow Windows Messenger to be run' (Not Scored)

Profile Applicability:

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

Description:

You can enable the setting for Do not allow Windows Messenger to be run to disable Windows Messenger and prevent the program from running. Note: This setting only affects Windows Messenger software included in Windows XP. This setting will not prevent users from running MSN Messenger or Windows Live Messenger.

Rationale:

Because this application has been used for malicious purposes such as spam, the distribution of malicious software, and disclosure of sensitive data, Microsoft recommends to enable this setting.

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\Software\Policies\Microsoft\Messenger\Client:PreventRun
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Windows Components\Windows
Messenger\Do not allow Windows Messenger to be run
```

Impact:

Users will be unable to use Windows Messenger.

1.2.3.4 Remote Desktop Services

1.2.3.4.1 Remote Desktop Connection Client

1.2.3.4.1.1 Configure 'Do not allow passwords to be saved' (Not Scored)

Profile Applicability:

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

Description:

This policy setting helps prevent Terminal Services clients from saving passwords on a computer. Note If this policy setting was previously configured as Disabled or Not configured, any previously saved passwords will be deleted the first time a Terminal Services 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 for your organization. This group policy object is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services:DisablePasswordSaving
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Windows Components\Remote Desktop
Services\Remote Desktop Connection Client\Do not allow passwords to be saved
```

Impact:

If you enable this policy setting, the password saving checkbox is disabled for Terminal Services clients and users will not be able to save passwords.

1.2.3.4.2 Remote Desktop Session Host

1.2.3.4.2.1 Device and Resource Redirection

1.2.3.4.2.1.1 Configure 'Do not allow drive redirection' (Not 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 Terminal 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.

Rationale:

Data could be forwarded from the user's Terminal Server session to the user's local computer without any direct user interaction.

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\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services:fDisableCdm
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Windows Components\Remote Desktop
Services\Remote Desktop Session Host\Device and Resource Redirection\Do not allow
drive redirection
```

Impact:

Drive redirection will not be possible.

1.2.3.4.2.2 Connections

1.2.3.4.2.2.1 Configure 'Allow users to connect remotely using Remote Desktop Services' (Not Scored)

Profile Applicability:

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

Description:

This policy setting allows you to control if users can connect to a computer using Terminal Services or Remote Desktop.

Rationale:

Any account with the Allow log on through Terminal Services user right can log on to the remote console of the computer. If you do not restrict access to legitimate users who need to log on to the console of the computer, unauthorized users could download and execute malicious code to elevate their privileges.

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\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:Not
Configured
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Windows Components\Remote Desktop
Services\Remote Desktop Session Host\Connections\Allow users to connect remotely using
Remote Desktop Services
```

Impact:

If this setting is enabled legitimate users will be unable to use Terminal Services or Remote Desktop, this could make it more difficult for help desk technicians to troubleshoot and resove problems remotely. It would also make it impossible to use Terminal Services for hosting shared applications.

1.2.3.4.2.3 Security

1.2.3.4.2.3.1 Configure 'Set client connection encryption level' (Not Scored)

Profile Applicability:

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

Description:

This policy setting specifies whether the computer that is about to host the remote connection will enforce an encryption level for all data sent between it and the client computer for the remote session.

Rationale:

If Terminal Server client connections are allowed that use low level encryption, it is more likely that an attacker will be able to decrypt any captured Terminal Services network traffic.

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\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services:MinEncryptionLevel
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Windows Components\Remote Desktop
Services\Remote Desktop Session Host\Security\Set client connection encryption level
```

Impact:

Clients that do not support 128-bit encryption will be unable to establish Terminal Server sessions.

1.2.3.4.2.3.2 Configure 'Always prompt for password upon connection' (Not Scored)

Profile Applicability:

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

Description:

This policy setting specifies whether Terminal 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 Terminal Services, even if they already provided

the password in the Remote Desktop Connection client. By default, Terminal Services allows users to automatically log on if they enter a password in the Remote Desktop Connection client. The Always prompt client for password upon connection setting is configured to Enabled for both of the environments that are discussed in this guide. Note If you do not configure this policy setting, the local computer administrator can use the Terminal Services Configuration tool to either allow or prevent passwords from being automatically sent.

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 Terminal 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 Terminal 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 for your organization. This group policy object is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services:fPromptForPassword
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Windows Components\Remote Desktop
Services\Remote Desktop Session Host\Security\Always prompt for password upon
connection
```

Impact:

Users will always have to enter their password when they establish new Terminal Server sessions.

1.2.3.5 Windows Error Reporting

1.2.3.5.1 Advanced Error Reporting Settings

1.2.3.5.1.1 Configure 'Report operating system errors' (Not Scored)

Profile Applicability:

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

Description:

This policy setting controls whether errors are reported. If you configure the Report Errors setting to Enabled, users have the ability to report errors when they occur. Errors can be reported to Microsoft through the Internet or to local file shares in the users' organizations. The possible values for the Report Errors setting are: . Enabled with options for: . Do not display links to any Microsoft provided more information Web sites. If you select this option, no links are displayed for Microsoft Web sites that may have more information about the error message. . Do not collect additional files. If you select this option, no additional files are collected to include in error reports. . Do not collect additional machine data. If you select this option, no additional information about the computer on which the error occurred is included in error reports. . Force queue mode for application errors. If you select this option, users do not have an option to send an error report. Instead, the error is placed in a queue directory, and the next administrator who logs on to the computer decides whether to report the error. . Corporate upload file path. You can select this option to specify a Universal Naming Convention (UNC) path to a file share where error reports are uploaded. This option also enables the Corporate Error Reporting tool. . Replace instances of the word Microsoft. If you select this option, you can customize the error reporting dialog boxes with your organization's name. . Disabled . Not Configured If you do not configure this policy setting, users cannot adjust the setting in the Control Panel. The default configuration is Enabled in Windows XP Professional and Disabled in Windows Server 2003. If the Report Errors setting is enabled, it will override any settings that are made through the Control Panel for error reporting. This configuration will also enforce the default values for any error reporting policies that are not configured.

Rationale:

In its default configuration, the Windows Corporate Error Reporting features of Windows XP and Office will send data to Microsoft that some organizations may prefer to keep confidential. The Microsoft privacy statement for Windows Corporate Error Reporting ensures that Microsoft will not misuse data that is collected through Windows Corporate

Error Reporting. However, some organizations may want to configure this feature so that no information is transmitted outside of the organization without first being reviewed by a trusted member of the IT team. Conversely, if error reporting is disabled completely, it is more difficult for Microsoft to identify and diagnose new bugs. Organizations that develop their own internal business applications can also take advantage of Windows Corporate Error Reporting to track down problems within their code. A reasonable configuration that ensures privacy and uses Windows Corporate Error Reporting effectively is to set up your own internal Corporate Error Reporting (CER) servers. Configure your client computers to point to these servers when they have error reports to submit. An administrator can then review the reports on the CER server and generate an aggregate report for Microsoft that contains no confidential information.

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\Software\Policies\Microsoft\PCHealth\ErrorReporting:IncludeKernelFaults
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Windows Components\Windows Error Reporting\Advanced Error Reporting Settings\Report operating system errors
```

Impact:

Error reporting will be enabled, and new error reports will be sent to the CER server.

1.2.3.5.2 Configure 'Display Error Notification' (Not Scored)

Profile Applicability:

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

Description:

You can use this policy setting to control whether or not a user may report an error. When this policy setting is enabled, the user will be notified that an error has occurred and provided with access to details about the error. If the Report Errors setting is also enabled,

the user will also be provided with a choice of whether to report the error. If you do not enable the Display Error Notification setting, the user is not provided with a choice of whether to report errors. If you enable the Report Errors setting errors will be automatically reported, but the user will not be notified when they occur. It is useful to disable this setting for server computers that do not have interactive users. If you do not configure this setting, users can adjust it through the Control Panel, which is set to Enable notification by default in Windows XP and Disable notification in Windows Server 2003.

Rationale:

If they are provided with the choice of whether or not to report errors, users may not comply with your organization's guidelines on error reporting. If you configure this policy setting to Disabled, users will not see error report messages.

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\Software\Policies\Microsoft\PCHealth\ErrorReporting:ShowUI
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Windows Components\Windows Error
Reporting\Display Error Notification
```

Impact:

Users will not see error report messages when they are generated.

1.2.3.6 NetMeeting

1.2.3.6.1 Configure 'Disable remote Desktop Sharing' (Not Scored)

Profile Applicability:

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

Description:

This policy setting disables the remote desktop sharing feature of NetMeeting. If you enable this policy setting, users will not be able to configure NetMeeting to allow remote control of the local desktop.

Rationale:

When this policy setting is enabled, users will not be able to use the remote desktop sharing feature of NetMeeting.

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\:Not Configured
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Windows Components\NetMeeting\Disable
remote Desktop Sharing
```

Impact:

Users will be unable to configure remote desktop sharing through NetMeeting, although they may still be able to use the Windows Remote Assistance and Remote Desktop features if you have left them enabled.

1.2.3.7 Windows Installer

1.2.3.7.1 Set 'Always install with elevated privileges' to 'Disabled' (Scored)

Profile Applicability:

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

Description:

Directs Windows Installer to use system permissions when it installs any program on the system. This setting extends elevated privileges to all programs. These privileges are usually reserved for programs that have been assigned to the user (offered on the desktop), assigned to the computer (installed automatically), or made available in Add or Remove Programs in Control Panel. This setting lets users install programs that require access to directories that the user might not have permission to view or change, including directories on highly restricted computers. If you disable this setting or do not configure it, the system applies the current user's permissions when it installs programs that a system administrator does not distribute or offer. 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: 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.

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 object is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer:AlwaysInstallElevated
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Windows
Installer\Always install with elevated privileges
```

Impact:

Windows Installer will apply the current user's permissions when it installs programs, this will prevent standard users from installing applications that affect system-wide configuration items.

1.2.3.8 Credential User Interface

1.2.3.8.1 Configure 'Require trusted path for credential entry.' (Not Scored)

Profile Applicability:

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

Description:

If you enable this policy setting, users are required to enter Windows credentials on the Secure Desktop by means of the trusted path mechanism. This means that before entering account and password information to authorize an elevation request, a user first need to press CTRL+ALT+DEL.

Rationale:

Requiring the use of a trusted path helps prevent a Trojan horse or other types of malicious code from stealing the user's Windows credentials.

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\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\CredUI:EnableSec
ureCredentialPrompting
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Administrative Templates\Windows Components\Credential User
Interface\Require trusted path for credential entry.
```

Impact:

If you disable or do not configure this policy setting, users can enter Windows credentials within the user's desktop session, potentially allowing malicious code access to the user's Windows credentials.

Appendix: Change History

Date	Version	Changes for this version
09-03-2004	1.0	Initial release to public
10-14-2004	1.0.2	Corrected document value of 3.2.1.67 MSS: AFD MaximumDynamicBacklog from 2000 to 20000.
10-20-2004	1.1	Renamed "High Security" to "Specialized Security - Limited Functionality"
10-18-2005	1.2	Corrected numbering errors in section 2 of the benchmark so that they correctly reflect numbering in section 1
10-18-2005	1.2	Altered descriptive text in several sections for accuracy and completeness
11-01-2007	1.3	Reformatted document be more inline with style guide
06-30-2009	2.1	Resovled bug 409, 448, 450, 473, 483, 363, 369.
10-01-2013	3.0	Ground-up rewrite of the benchmark.