Solutions for Security and Compliance

Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP

Version 2.0

Published: December 2005
For the latest information, please see www.microsoft.com/technet/security
Contents

Feedback .................................................................................................................................................. xxix

Chapter 1: Introduction to Threats and Countermeasures: Security
Settings in Windows Server 2003 and Windows XP ................................................................. 1

Chapter Summaries ................................................................................................................................. 4

Chapter 1: Introduction to Threats and Countermeasures: Security
Settings in Windows Server 2003 and Windows XP ................................................................. 4
Chapter 2: Domain Level Policies ....................................................................................................... 4
Chapter 3: Audit Policy ........................................................................................................................... 4
Chapter 4: User Rights ............................................................................................................................ 4
Chapter 5: Security Options .................................................................................................................. 4
Chapter 6: Event Log ............................................................................................................................... 4
Chapter 7: System Services .................................................................................................................... 4
Chapter 8: Software Restriction Policies .............................................................................................. 5
Chapter 9: Windows XP and Windows Server 2003 Administrative
Templates .............................................................................................................................................. 5
Chapter 10: Additional Registry Entries ............................................................................................... 5
Chapter 11: Additional Countermeasures ............................................................................................. 5
Chapter 12: Conclusion ........................................................................................................................... 5

Tools and Templates ................................................................................................................................. 6

Chapter 2: Domain Level Policies ......................................................................................................... 7

Account Policies ....................................................................................................................................... 7

Password Policy ....................................................................................................................................... 8
  Enforce password history ..................................................................................................................... 8
  Maximum password age ....................................................................................................................... 10
  Minimum password age ....................................................................................................................... 10
  Minimum password length ................................................................................................................... 11
  Passwords must meet complexity requirements .................................................................................. 12
  Store password using reversible encryption for all users in the domain .............................................. 13
Account Lockout Policy ........................................................................................................................... 14
  Account lockout duration .................................................................................................................... 15
  Account lockout threshold .................................................................................................................. 15
  Reset account lockout counter after .................................................................................................. 17
Kerberos Policy ........................................................................................................................................ 18
  Enforce user logon restrictions ........................................................................................................... 18
  Maximum lifetime for service ticket ................................................................................................. 18
Threats and Countermeasures

Maximum lifetime for user ticket ........................................ 19
Maximum lifetime for user ticket renewal ................................ 19
Maximum tolerance for computer clock synchronization .............. 20

More Information .................................................................. 21

Chapter 3: Audit Policy ............................................................ 23
Audit Settings ........................................................................ 25
Audit account logon events ....................................................... 25
Audit account management ...................................................... 26
Audit directory service access ................................................... 26
Audit logon events .................................................................. 26
Audit object access .................................................................. 26
Audit policy change ................................................................. 27
Audit privilege use ................................................................... 27
Audit process tracking .............................................................. 29
Audit system events ................................................................. 29

Audit Example: Results of a User Logon Event ......................... 30
User logs on to their computer .................................................. 30
User connects to the shared folder called Share ......................... 30
User opens the file document.txt ............................................. 31
User saves the file document.txt .............................................. 31

More Information .................................................................. 32

Chapter 4: User Rights ............................................................. 33
User Rights Assignment Settings ............................................. 33
Access this computer from the network ..................................... 33
Vulnerability .......................................................................... 34
Countermeasure ..................................................................... 34
Potential Impact ...................................................................... 34
Act as part of the operating system .......................................... 34
Vulnerability .......................................................................... 34
Countermeasure ..................................................................... 35
Potential Impact ...................................................................... 35
Add workstations to domain ...................................................... 35
Vulnerability .......................................................................... 35
Countermeasure ..................................................................... 35
Potential Impact ...................................................................... 35
Adjust memory quotas for a process ......................................... 36
Threats and Countermeasures

Vulnerability ........................................................................................................... 36
Countermeasure ..................................................................................................... 36
Potential Impact ..................................................................................................... 36
Allow log on locally ................................................................................................. 36
Vulnerability ........................................................................................................... 36
Countermeasure ..................................................................................................... 37
Potential Impact ..................................................................................................... 37
Allow log on through Terminal Services ............................................................... 37
Vulnerability ........................................................................................................... 37
Countermeasure ..................................................................................................... 37
Potential Impact ..................................................................................................... 38
Back up files and directories .................................................................................. 38
Vulnerability ........................................................................................................... 38
Countermeasure ..................................................................................................... 38
Potential Impact ..................................................................................................... 38
Bypass traverse checking ....................................................................................... 38
Vulnerability ........................................................................................................... 39
Countermeasure ..................................................................................................... 39
Potential Impact ..................................................................................................... 39
Change the system time ......................................................................................... 39
Vulnerability ........................................................................................................... 39
Countermeasure ..................................................................................................... 40
Potential Impact ..................................................................................................... 40
Create a page file .................................................................................................... 40
Vulnerability ........................................................................................................... 40
Countermeasure ..................................................................................................... 40
Potential Impact ..................................................................................................... 40
Create a token object ............................................................................................. 41
Vulnerability ........................................................................................................... 41
Countermeasure ..................................................................................................... 41
Potential Impact ..................................................................................................... 41
Create global objects ............................................................................................. 41
Vulnerability ........................................................................................................... 41
Countermeasure ..................................................................................................... 41
Potential Impact ..................................................................................................... 41
Create permanent shared objects ........................................................................ 42
Vulnerability ........................................................................................................... 42
Countermeasure ..................................................................................................... 42
Threats and Countermeasures

Potential Impact .......................................................... 42
Debug programs ............................................................. 42
Vulnerability ................................................................. 42
Countermeasure ............................................................. 42
Potential Impact ............................................................. 42
Deny access to this computer from the network ......................... 43
Vulnerability ................................................................. 43
Countermeasure ............................................................. 43
Potential Impact ............................................................. 44
Deny log on as a batch job .................................................. 44
Vulnerability ................................................................. 44
Countermeasure ............................................................. 44
Potential Impact ............................................................. 44
Deny log on as a service .................................................... 45
Vulnerability ................................................................. 45
Countermeasure ............................................................. 45
Potential Impact ............................................................. 45
Deny log on locally .......................................................... 45
Vulnerability ................................................................. 45
Countermeasure ............................................................. 46
Potential Impact ............................................................. 46
Deny log on through Terminal Services ................................. 46
Vulnerability ................................................................. 46
Countermeasure ............................................................. 46
Potential Impact ............................................................. 46
Enable computer and user accounts to be trusted for delegation .... 47
Vulnerability ................................................................. 47
Countermeasure ............................................................. 47
Potential Impact ............................................................. 47
Force shutdown from a remote system .................................. 47
Vulnerability ................................................................. 47
Countermeasure ............................................................. 48
Potential Impact ............................................................. 48
Generate security audits ..................................................... 48
Vulnerability ................................................................. 48
Countermeasure ............................................................. 48
Potential Impact ............................................................. 48
Impersonate a client after authentication ............................... 48
<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Countermeasure</th>
<th>Potential Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increase scheduling priority</td>
<td>49</td>
<td></td>
</tr>
<tr>
<td>Load and unload device drivers</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td>Lock pages in memory</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td>Log on as a batch job</td>
<td>51</td>
<td></td>
</tr>
<tr>
<td>Log on as a service</td>
<td>52</td>
<td></td>
</tr>
<tr>
<td>Manage auditing and security log</td>
<td>52</td>
<td></td>
</tr>
<tr>
<td>Modify firmware environment values</td>
<td>53</td>
<td></td>
</tr>
<tr>
<td>Perform volume maintenance tasks</td>
<td>53</td>
<td></td>
</tr>
<tr>
<td>Profile single process</td>
<td>54</td>
<td></td>
</tr>
</tbody>
</table>
Potential Impact ................................................................. 54
Profile system performance .............................................. 54
Vulnerability ..................................................................... 54
Countermeasure ............................................................... 55
Potential Impact ............................................................... 55
Remove computer from docking station ................................. 55
Vulnerability ..................................................................... 55
Countermeasure ............................................................... 55
Potential Impact ............................................................... 55
Replace a process level token ................................................ 56
Vulnerability ..................................................................... 56
Countermeasure ............................................................... 56
Potential Impact ............................................................... 56
Restore files and directories .................................................. 56
Vulnerability ..................................................................... 56
Countermeasure ............................................................... 57
Potential Impact ............................................................... 57
Shut down the system .......................................................... 57
Vulnerability ..................................................................... 57
Countermeasure ............................................................... 57
Potential Impact ............................................................... 57
Synchronize directory service data .......................................... 57
Vulnerability ..................................................................... 58
Potential Impact ............................................................... 58
Take ownership of files or other objects ................................. 58
Vulnerability ..................................................................... 58
Countermeasure ............................................................... 58
Potential Impact ............................................................... 58

More Information .................................................................. 59

Chapter 5: Security Options ................................................... 61
Security Options Settings ...................................................... 61
Accounts: Administrator account status ................................. 61
Vulnerability ..................................................................... 61
Countermeasure ............................................................... 62
Potential Impact ............................................................... 62
Accounts: Guest account status ............................................. 62
Vulnerability ..................................................................... 62
Threats and Countermeasures

Countermeasure ................................................................. 62
Potential Impact ................................................................. 62
Accounts: Limit local account use of blank passwords to console logon only .... 63
Vulnerability ........................................................................ 63
Countermeasure ................................................................. 63
Potential Impact ................................................................. 63
Accounts: Rename administrator account .................................. 63
Vulnerability ........................................................................ 63
Countermeasure ................................................................. 64
Potential Impact ................................................................. 64
Accounts: Rename guest account .......................................... 64
Vulnerability ........................................................................ 64
Countermeasure ................................................................. 64
Potential Impact ................................................................. 64
Audit: Audit the access of global system objects ....................... 65
Vulnerability ........................................................................ 65
Countermeasure ................................................................. 65
Potential Impact ................................................................. 65
Audit: Audit the use of Backup and Restore privilege ............... 65
Vulnerability ........................................................................ 66
Countermeasure ................................................................. 66
Potential Impact ................................................................. 66
Audit: Shut down system immediately if unable to log security audits .. 66
Vulnerability ........................................................................ 67
Countermeasure ................................................................. 67
Potential Impact ................................................................. 67
DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) ................................................... 67
Vulnerability ........................................................................ 68
Countermeasure ................................................................. 68
To protect individual COM-based applications or services, set the .......... 68
Potential Impact ................................................................. 68
DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) ................................................... 69
Vulnerability ........................................................................ 69
Countermeasure ................................................................. 69
To protect individual COM-based applications or services, set the .......... 69
Potential Impact ................................................................. 70
Devices: Allow undock without having to log on .......................... 70
<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Countermeasure</th>
<th>Potential Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Devices: Allowed to format and eject removable media</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Devices: Prevent users from installing printer drivers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Devices: Restrict CD-ROM access to locally logged-on user only</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Devices: Restrict floppy access to locally logged-on user only</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Devices: Unsigned driver installation behavior</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Domain controller: Allow server operators to schedule tasks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Domain controller: LDAP server signing requirements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Domain controller: Refuse machine account password changes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Domain member: Digitally encrypt or sign secure channel data (multiple related settings)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Countermeasure ................................................................. 77
Potential Impact .................................................................. 77
Domain member: Disable machine account password changes .............. 78
Vulnerability ...................................................................... 78
Countermeasure .................................................................. 79
Potential Impact .................................................................. 79
Domain member: Maximum machine account password age .................. 79
Vulnerability ...................................................................... 79
Countermeasure .................................................................. 79
Potential Impact .................................................................. 79
Domain member: Require strong (Windows 2000 or later) session key ...... 79
Vulnerability ...................................................................... 80
Countermeasure .................................................................. 80
Potential Impact .................................................................. 80
Interactive logon: Do not display last user name .................................. 80
Vulnerability ...................................................................... 81
Countermeasure .................................................................. 81
Potential Impact .................................................................. 81
Interactive logon: Do not require CTRL+ALT+DEL .............................. 81
Vulnerability ...................................................................... 81
Countermeasure .................................................................. 81
Potential Impact .................................................................. 81
Interactive logon: Message text for users attempting to log on ................ 82
Vulnerability ...................................................................... 82
Countermeasure .................................................................. 82
Potential Impact .................................................................. 82
Interactive logon: Number of previous logons to cache (in case domain controller is not available) .............................................................. 82
Vulnerability ...................................................................... 83
Countermeasure .................................................................. 83
Potential Impact .................................................................. 83
Interactive logon: Prompt user to change password before expiration ........ 83
Vulnerability ...................................................................... 84
Countermeasure .................................................................. 84
Potential Impact .................................................................. 84
Interactive logon: Require Domain Controller authentication to unlock workstation .................................................................................................. 84
Vulnerability ...................................................................... 84
Countermeasure .................................................................. 85
Potential Impact ................................................................. 85
Interactive logon: Require smart card ...................................... 85
Vulnerability ........................................................................ 85
Countermeasure .................................................................. 85
Potential Impact .................................................................. 86
Interactive logon: Smart card removal behavior ...................... 86
Vulnerability ........................................................................ 86
Countermeasure .................................................................. 86
Potential Impact .................................................................. 86
Microsoft network client and server: Digitally sign communications (four related settings) .......................................................... 87
Vulnerability ........................................................................ 87
Countermeasure .................................................................. 87
Potential Impact .................................................................. 87
Microsoft network client: Send unencrypted password to third-party SMB servers ............................................................................ 88
Vulnerability ........................................................................ 88
Countermeasure .................................................................. 88
Potential Impact .................................................................. 88
Microsoft network server: Amount of idle time required before suspending session ................................................................. 88
Vulnerability ........................................................................ 89
Countermeasure .................................................................. 89
Potential Impact .................................................................. 89
Microsoft network server: Disconnect clients when logon hours expire ......................................................................................... 89
Vulnerability ........................................................................ 89
Countermeasure .................................................................. 89
Potential Impact .................................................................. 90
Network access: Allow anonymous SID/Name translation ............ 90
Vulnerability ........................................................................ 90
Countermeasure .................................................................. 90
Potential Impact .................................................................. 90
Network access: Do not allow anonymous enumeration of SAM accounts ............................................................... 90
Vulnerability ........................................................................ 91
Countermeasure .................................................................. 91
Potential Impact .................................................................. 91
Network access: Do not allow anonymous enumeration of SAM accounts and shares ............................................................ 91
Vulnerability ........................................................................ 92
Countermeasure .................................................................. 92
<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Countermeasure</th>
<th>Potential Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network access: Do not allow storage of credentials or .NET Passports for network authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network access: Let Everyone permissions apply to anonymous users</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network access: Named Pipes that can be accessed anonymously</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network access: Remotely accessible registry paths</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network access: Remotely accessible registry paths and sub-paths</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network access: Restrict anonymous access to Named Pipes and Shares</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network access: Shares that can be accessed anonymously</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network access: Sharing and security model for local accounts</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network security: Do not store LAN Manager hash value on next password change</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Network security: Force logoff when logon hours expire
Vulnerability
Countermeasure
Potential Impact

Network security: LAN Manager authentication level
Vulnerability
Countermeasure
Potential Impact

Network security: LDAP client signing requirements
Vulnerability
Countermeasure
Potential Impact

Network security: Minimum session security for NTLM SSP based (including secure RPC) clients
Vulnerability
Countermeasure
Potential Impact

Network security: Minimum session security for NTLM SSP based (including secure RPC) servers
Vulnerability
Countermeasure
Potential Impact

Recovery console: Allow automatic administrative logon
Vulnerability
Countermeasure
Potential Impact

Recovery console: Allow floppy copy and access to all drives and all folders
Vulnerability
Countermeasure
Potential Impact

Shutdown: Allow system to be shut down without having to log on
Vulnerability
Countermeasure
Potential Impact

Shutdown: Clear virtual memory page file
Vulnerability
Countermeasure
Potential Impact
System cryptography: Force strong key protection for user keys stored on the computer ................................................. 107
Vulnerability ........................................................................ 107
Countermeasure .................................................................. 107
Potential Impact .................................................................. 107

System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing ........................................... 108
Vulnerability ........................................................................ 108
Countermeasure .................................................................. 109
Potential Impact .................................................................. 108

System objects: Default owner for objects created by members of the Administrators group ............................................ 109
Vulnerability ........................................................................ 109
Countermeasure .................................................................. 109
Potential Impact .................................................................. 109

System objects: Require case insensitivity for non-Windows subsystems ................................................................. 110
Vulnerability ........................................................................ 110
Countermeasure .................................................................. 110
Potential Impact .................................................................. 110

System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links) ................................. 111
Vulnerability ........................................................................ 111
Countermeasure .................................................................. 111
Potential Impact .................................................................. 111

System settings: Optional subsystems ........................................... 111
Vulnerability ........................................................................ 111
Countermeasure .................................................................. 112
Potential Impact .................................................................. 112

Vulnerability ........................................................................ 112
Countermeasure .................................................................. 112
Potential Impact .................................................................. 112

More Information ........................................................................................................... 113

Chapter 6: Event Log .............................................................................................................. 115
Event Log Settings .............................................................................................................. 115
Maximum event log size ................................................................................................. 115
Vulnerability ........................................................................ 115
Countermeasure .................................................................. 116
Potential Impact .................................................................116
Prevent local guests group from accessing event logs .............117
Vulnerability ...........................................................................117
Countermeasure .................................................................117
Potential Impact .................................................................117
Retain event logs ..................................................................117
Vulnerability ...........................................................................118
Countermeasure .................................................................118
Potential Impact .................................................................118
Retention method for event log ............................................118
Vulnerability ...........................................................................119
Countermeasure .................................................................119
Potential Impact .................................................................119
Delegating Access to the Event Logs ....................................120

More Information ..................................................................121

Chapter 7: System Services ....................................................123
Services Overview ...............................................................124
Vulnerability ...........................................................................124
Countermeasure .................................................................125
Potential Impact .................................................................125
Do Not Set Permissions on Service Objects ...............................126
Manually Editing Security Templates ......................................127
Descriptions of System Services ............................................129
Alerter .....................................................................................129
Application Experience Lookup Service ................................129
Application Layer Gateway Service .......................................129
Application Management ......................................................130
ASP .NET State Service .......................................................130
Automatic Updates ................................................................131
Background Intelligent Transfer Service (BITS) ......................131
Certificate Services .............................................................132
Client Service for NetWare ....................................................132
ClipBook ...............................................................................132
Cluster Service ......................................................................133
COM+ Event System ............................................................133
COM+ System Application ...................................................134
Computer Browser ..............................................................134
 threat and countermeasures

Cryptography Services ................................................................. 134
DCOM Server Process Launcher .................................................... 135
DHCP Client .............................................................................. 135
DHCP Server ............................................................................. 136
Distributed File System ................................................................. 136
Distributed Link Tracking Client .................................................... 137
Distributed Link Tracking Server ................................................... 137
Distributed Transaction Coordinator .............................................. 138
DNS Client ................................................................................. 138
DNS Server ............................................................................... 139
Error Reporting Service ................................................................. 139
Event Log ................................................................................... 140
Fast User Switching Compatibility ................................................ 141
Fax Service .................................................................................. 141
File Replication .......................................................................... 142
File Server for Macintosh ............................................................... 142
FTP Publishing Service ................................................................. 142
Help and Support ....................................................................... 142
HTTP SSL .................................................................................... 143
Human Interface Device Access ..................................................... 143
IAS Jet Database Access ................................................................. 143
IIS Admin Service ........................................................................ 144
IMAPI CD-Burning COM Service .................................................. 144
Indexing Service ......................................................................... 144
Infrared Monitor .......................................................................... 144
Internet Authentication Service ..................................................... 145
Intersite Messaging ..................................................................... 145
IP Version 6 Helper Service .......................................................... 145
IPSec Policy Agent (IPSec Service) ............................................... 146
Kerberos Key Distribution Center .................................................. 146
License Logging Service ................................................................. 146
Logical Disk Manager ................................................................. 147
Logical Disk Manager Administrative Service ............................... 147
Machine Debug Manager .............................................................. 147
Message Queuing ........................................................................ 148
Message Queuing Down Level Clients ......................................... 148
Message Queuing Triggers ............................................................ 149
Messenger .................................................................................... 149
Microsoft POP3 Service ................................................................. 149
Microsoft Software Shadow Copy Provider .................................. 149
MSSQL$UDDI .................................................................................. 150
MSSQLServerADHelper ................................................................. 151
.NET Framework Support Service ................................................. 151
Net Logon ...................................................................................... 151
NetMeeting Remote Desktop Sharing .......................................... 152
Network Connections .................................................................. 152
Network DDE ................................................................................ 152
Network DDE DSDM ..................................................................... 153
Network Location Awareness (NLA) ............................................. 153
Network Provisioning Service ...................................................... 153
Network News Transfer Protocol (NNTP) ..................................... 154
NTLM Security Support Provider ................................................ 154
Performance Logs and Alerts ...................................................... 155
Plug and Play .............................................................................. 155
Portable Media Serial Number .................................................... 155
Print Server for Macintosh ......................................................... 156
Print Spooler ................................................................................ 156
Protected Storage ....................................................................... 156
QoS RSVP Service ....................................................................... 157
Remote Access Auto Connection Manager .................................. 157
Remote Access Connection Manager .......................................... 157
Remote Administration Service ................................................... 158
Remote Desktop Help Session Manager ...................................... 158
Remote Installation ..................................................................... 158
Remote Procedure Call (RPC) ...................................................... 159
Remote Procedure Call (RPC) Locator ........................................ 159
Remote Registry Service ............................................................. 159
Remote Server Manager .............................................................. 160
Remote Server Monitor ............................................................... 160
Remote Storage Notification ....................................................... 160
Remote Storage Server ............................................................... 160
Removable Storage .................................................................... 161
Resultant Set of Policy Provider ................................................ 161
Routing and Remote Access ...................................................... 161
SAP Agent ................................................................................... 162
Secondary Logon ....................................................................... 162
<table>
<thead>
<tr>
<th>Service Name</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Accounts Manager</td>
<td>162</td>
</tr>
<tr>
<td>Security Center</td>
<td>163</td>
</tr>
<tr>
<td>Server</td>
<td>163</td>
</tr>
<tr>
<td>Shell Hardware Detection</td>
<td>163</td>
</tr>
<tr>
<td>Simple Mail Transport Protocol (SMTP)</td>
<td>164</td>
</tr>
<tr>
<td>Simple TCP/IP Services</td>
<td>164</td>
</tr>
<tr>
<td>Single Instance Storage Groveler</td>
<td>165</td>
</tr>
<tr>
<td>Smart Card</td>
<td>165</td>
</tr>
<tr>
<td>SNMP Service</td>
<td>165</td>
</tr>
<tr>
<td>SNMP Trap Service</td>
<td>166</td>
</tr>
<tr>
<td>Special Administration Console Helper</td>
<td>167</td>
</tr>
<tr>
<td>SQLAgent$* (* UDDI or WebDB)</td>
<td>167</td>
</tr>
<tr>
<td>SSDP Discovery Service</td>
<td>167</td>
</tr>
<tr>
<td>System Event Notification</td>
<td>168</td>
</tr>
<tr>
<td>System Restore Service</td>
<td>168</td>
</tr>
<tr>
<td>Task Scheduler</td>
<td>168</td>
</tr>
<tr>
<td>TCP/IP NetBIOS Helper Service</td>
<td>169</td>
</tr>
<tr>
<td>TCP/IP Print Server</td>
<td>169</td>
</tr>
<tr>
<td>Telephony</td>
<td>169</td>
</tr>
<tr>
<td>Telnet</td>
<td>170</td>
</tr>
<tr>
<td>Terminal Services</td>
<td>170</td>
</tr>
<tr>
<td>Terminal Services Licensing</td>
<td>170</td>
</tr>
<tr>
<td>Terminal Services Session Directory</td>
<td>170</td>
</tr>
<tr>
<td>Themes</td>
<td>170</td>
</tr>
<tr>
<td>Trivial FTP Daemon</td>
<td>171</td>
</tr>
<tr>
<td>Uninterruptible Power Supply</td>
<td>172</td>
</tr>
<tr>
<td>Universal Plug and Play Device Host</td>
<td>172</td>
</tr>
<tr>
<td>Upload Manager</td>
<td>172</td>
</tr>
<tr>
<td>Virtual Disk Service</td>
<td>172</td>
</tr>
<tr>
<td>Volume Shadow Copy</td>
<td>173</td>
</tr>
<tr>
<td>WebClient</td>
<td>173</td>
</tr>
<tr>
<td>Web Element Manager</td>
<td>173</td>
</tr>
<tr>
<td>Windows Audio</td>
<td>174</td>
</tr>
<tr>
<td>Windows Firewall /Internet Connection Sharing</td>
<td>175</td>
</tr>
<tr>
<td>Windows Image Acquisition (WIA)</td>
<td>175</td>
</tr>
<tr>
<td>Windows Installer</td>
<td>175</td>
</tr>
<tr>
<td>Windows Internet Name Service (WINS)</td>
<td>176</td>
</tr>
<tr>
<td>Windows Management Instrumentation</td>
<td>176</td>
</tr>
</tbody>
</table>
Windows Management Instrumentation Driver Extensions ...................... 177
Windows Media Services ........................................................................ 177
Windows System Resource Manager ......................................................... 177
Windows Time ......................................................................................... 178
WinHTTP Web Proxy Auto-Discovery Service ........................................ 179
Wireless Configuration ............................................................................. 179
WMI Performance Adapter ....................................................................... 179
Workstation ............................................................................................ 180
World Wide Web Publishing Service ....................................................... 180

More Information .................................................................................... 181

Chapter 8: Software Restriction Policies .................................................. 183
The Threat of Malicious Software .............................................................. 183
Vulnerability ............................................................................................. 183
Countermeasure ....................................................................................... 183
Potential Impact ....................................................................................... 184

More Information .................................................................................... 184

Chapter 9: Windows XP and Windows Server 2003 Administrative
Templates .................................................................................................. 185
Computer Configuration Settings ............................................................... 186
NetMeeting ................................................................................................. 186
  Disable remote Desktop Sharing .............................................................. 186
Internet Explorer Computer Settings ......................................................... 186
  Disable Automatic Install of Internet Explorer components ................ 187
  Disable Periodic Check for Internet Explorer software updates .......... 187
  Disable software update shell notifications on program launch ......... 188
  Make proxy settings per-machine (rather than per-user) .................... 189
  Security Zones: Do not allow users to add/delete sites ...................... 189
  Security Zones: Do not allow users to change policies ...................... 190
  Security Zones: Use only machine settings ...................................... 190
  Turn off Crash Detection .................................................................... 191
  Do not allow users to enable or disable add-ons ............................... 191
Internet Explorer\Internet Control Panel\Security Page ......................... 193
  Vulnerability ......................................................................................... 193
  Countermeasure ................................................................................... 193
  Potential Impact ................................................................................... 193
Internet Explorer\Internet Control Panel\Advanced Page ...................... 193
Allow software to run or install even if the signature is invalid ..................193
Allow active content from CDs to run on user machines .........................194
Allow third-party browser extensions ............................................195
Check for server certificate revocation ...........................................195
Check for signatures on downloaded programs ..................................196
Do not save encrypted pages to disk .............................................196
Empty Temporary Internet Files folder when browser is closed ..............197

Internet Explorer\Security Features ..............................................197
Binary Behavior Security Restriction ............................................198
MK Protocol Security Restriction ..................................................198
Local Machine Zone Lockdown Security .......................................199
Consistent MIME Handling .........................................................199
MIME Sniffing Safety Features ....................................................200
Object Caching Protection ..........................................................200
Scripted Window Security Restrictions .........................................201
Protection From Zone Elevation ...................................................201
Restrict ActiveX Install ..............................................................202
Restrict File Download ..............................................................202
Add-on Management .................................................................203
Network Protocol Lockdown ..........................................................203

Internet Information Services .........................................................204
Prevent IIS installation ...............................................................204

Terminal Services ........................................................................205
Deny log off of an administrator logged in to the console session ..........205
Do not allow local administrators to customize permissions .................206
Sets rules for remote control of Terminal Services user sessions ..........207

Client/Server Data Redirection ........................................................208
Allow Time Zone Redirection .........................................................208
Do not allow clipboard redirection ................................................209
Allow audio redirection ................................................................209
Do not allow COM port redirection ...............................................210
Do not allow client printer redirection ............................................210
Do not allow LPT port redirection ..................................................211
Do not allow drive redirection .......................................................211
Do not set default client printer to be default printer in a session ..........212

Encryption and Security .................................................................213
Set Client Connection Encryption Level ........................................213
Always prompt client for a password on connection ..........................214
RPC Security Policy ................................................................. 215
  Secure Server (Require Security) ............................................. 215
Sessions .................................................................................. 216
  Set time limit for disconnected sessions .................................. 216
  Allow reconnection from original client only .......................... 217
Windows Explorer ................................................................. 218
  Turn off shell protocol protected mode .................................. 218
Windows Messenger .............................................................. 218
  Do not allow Windows Messenger to be run ............................ 219
Windows Update ..................................................................... 220
  Configure Automatic Updates .................................................. 220
  No auto-restart for scheduled Automatic Updates installations ...... 221
  Reschedule Automatic Updates scheduled installations .............. 222
  Specify intranet Microsoft update service location .................... 222
System .................................................................................. 223
  Turn off Autoplay .................................................................. 223
Logon ..................................................................................... 224
  Don’t display the Getting Started welcome screen at logon .......... 224
  Do not process the legacy run list .......................................... 225
  Do not process the run once list ............................................ 225
Group Policy .......................................................................... 226
  Internet Explorer Maintenance policy processing ..................... 226
  IP security policy processing ................................................. 227
  Registry policy processing .................................................... 228
  Security policy processing ..................................................... 229
Remote Assistance ............................................................... 229
  Offer Remote Assistance ...................................................... 230
  Solicit Remote Assistance ..................................................... 230
Error Reporting ..................................................................... 232
  Display Error Notification ..................................................... 232
  Report Errors ...................................................................... 233
Internet Communications Management .................................... 234
Distributed COM .................................................................... 234
  Common Issues .................................................................. 235
  Allow local activation security check exemptions ..................... 235
  Define Activation Security Check exemptions ......................... 235
User Configuration Settings ..................................................... 237
  Internet Explorer User Settings ................................................ 237
Configure Outlook Express ..............................................................237
Disable Changing Advanced page settings ......................................237
Disable Changing Automatic Configuration Settings ..........................238
Disable Changing Certificate Settings ..............................................239
Disable Changing Connection Settings ..........................................239
Disable Changing Proxy Settings .................................................240
Disable Internet Connection Wizard ..............................................240
Do not allow AutoComplete to save passwords ................................241
Internet Control Panel ....................................................................242
  Disable the Advanced Page .........................................................242
  Disable the Security Page ............................................................242
Offline Pages ..............................................................................243
  Disable adding channels ..............................................................243
  Disable adding schedules for offline pages ....................................244
  Disable all scheduled offline pages .............................................244
  Disable channel user interface completely ...................................245
  Disable downloading of site subscription content ............................245
  Disable editing and creating of schedule groups ............................246
  Disable editing schedules for offline pages ....................................247
  Disable offline page hit logging ...................................................247
  Disable removing channels ..........................................................248
  Disable removing schedules for offline pages ...............................249
Browser Menus ...........................................................................250
  Disable Save this program to disk option ......................................250
Persistence Behavior .....................................................................250
Attachment Manager ....................................................................251
  Default risk level for file attachments .........................................252
  Inclusion list for high risk file types ............................................252
  Inclusion list for moderate risk file types .....................................253
  Inclusion list for low file types ....................................................253
  Trust logic for file attachments ..................................................254
  Do not preserve zone information in file attachments .....................255
  Hide mechanisms to remove zone information .............................255
  Notify antivirus programs when opening attachments ....................256
Windows Explorer .......................................................................257
  Remove CD Burning features .....................................................257
  Remove Security tab ...................................................................257
System .......................................................................................258
Prevent access to registry editing tools ........................................... 258
System\Power Management .......................................................... 258
Prompt for password on resume from hibernate / suspend .................. 258
Screen Saver Settings ..................................................................... 259
Hide Screen Saver tab ..................................................................... 259
Password protect the screen saver ................................................. 259
Screen Saver .................................................................................. 260
Screen Saver executable name ....................................................... 260
Screen Saver timeout ..................................................................... 260

Chapter 10: Additional Registry Entries ........................................... 265
Customized Security Configuration Editor ......................................... 265
How to Modify the Security Configuration Editor User Interface ........ 265
TCP/IP-Related Registry Entries ....................................................... 268
DisableIPSourceRouting: IP source routing protection level (protects
against packet spoofing) ................................................................ 268
Vulnerability .................................................................................. 269
Countermeasure ............................................................................ 269
Potential Impact ............................................................................ 269
EnableDeadGDetect: Allow automatic detection of dead network
gateways (could lead to DoS) ......................................................... 269
Vulnerability .................................................................................. 269
Countermeasure ............................................................................ 269
Potential Impact ............................................................................ 270
EnableICMPRedirect: Allow ICMP redirects to override OSPF generated
routes ........................................................................................... 270
Vulnerability .................................................................................. 270
Countermeasure ............................................................................ 270
Potential Impact ............................................................................ 270
KeepAliveTime: How often keep-alive packets are sent in milliseconds
(300,000 is recommended) ............................................................... 270
Vulnerability .................................................................................. 271
Countermeasure ............................................................................ 271
Potential Impact ............................................................................ 271
PerformRouterDiscovery: Allow IRDP to detect and configure Default
Gateway addresses (could lead to DoS) ........................................... 271
Vulnerability .................................................................................. 271
Countermeasure ............................................................................ 271
Potential Impact ............................................................................ 272
<table>
<thead>
<tr>
<th>Threats and Countermeasures</th>
</tr>
</thead>
<tbody>
<tr>
<td>SynAttackProtect: Syn attack protection level (protects against DoS)</td>
</tr>
<tr>
<td>Vulnerability</td>
</tr>
<tr>
<td>Countermeasure</td>
</tr>
<tr>
<td>Potential Impact</td>
</tr>
<tr>
<td>TcpMaxConnectResponseRetransmissions: SYN-ACK retransmissions when a connection request is not acknowledged</td>
</tr>
<tr>
<td>Vulnerability</td>
</tr>
<tr>
<td>Countermeasure</td>
</tr>
<tr>
<td>Potential Impact</td>
</tr>
<tr>
<td>TcpMaxDataRetransmissions: How many times unacknowledged data is retransmitted (3 recommended, 5 is default)</td>
</tr>
<tr>
<td>Vulnerability</td>
</tr>
<tr>
<td>Countermeasure</td>
</tr>
<tr>
<td>Potential Impact</td>
</tr>
<tr>
<td>Miscellaneous Registry Entries</td>
</tr>
<tr>
<td>Disable Automatic Logon: Disable Automatic Logon</td>
</tr>
<tr>
<td>Vulnerability</td>
</tr>
<tr>
<td>Countermeasure</td>
</tr>
<tr>
<td>Potential Impact</td>
</tr>
<tr>
<td>Configure Automatic Reboot from System Crashes</td>
</tr>
<tr>
<td>Vulnerability</td>
</tr>
<tr>
<td>Countermeasure</td>
</tr>
<tr>
<td>Potential Impact</td>
</tr>
<tr>
<td>Enable Administrative Shares</td>
</tr>
<tr>
<td>Vulnerability</td>
</tr>
<tr>
<td>Countermeasure</td>
</tr>
<tr>
<td>Potential Impact</td>
</tr>
<tr>
<td>Disable Saving of Dial-Up Passwords</td>
</tr>
<tr>
<td>Vulnerability</td>
</tr>
<tr>
<td>Countermeasure</td>
</tr>
<tr>
<td>Potential Impact</td>
</tr>
<tr>
<td>Hide the Computer from Network Neighborhood Browse Lists: Hide Computer From the Browse List</td>
</tr>
<tr>
<td>Vulnerability</td>
</tr>
<tr>
<td>Countermeasure</td>
</tr>
<tr>
<td>Potential Impact</td>
</tr>
<tr>
<td>Enable IPSec to protect Kerberos RSVP Traffic: Enable NoDefaultExempt for IPSec Filtering</td>
</tr>
<tr>
<td>Vulnerability</td>
</tr>
<tr>
<td>Countermeasure</td>
</tr>
</tbody>
</table>
Threats and Countermeasures

Potential Impact .................................................................281
Disable Autorun: Disable Autorun for all drives ..........................281
Vulnerability .........................................................................282
Countermeasure ....................................................................282
Potential Impact ....................................................................282

Configure NetBIOS Name Release Security: (NoNameReleaseOnDemand)
Allow the computer to ignore NetBIOS name release requests except from
WINS servers ........................................................................282
Vulnerability .........................................................................283
Countermeasure ....................................................................283
Potential Impact ....................................................................283

Disable Auto Generation of 8.3 File Names: Enable the computer to stop
generating 8.3 style filenames .................................................284
Vulnerability .........................................................................284
Countermeasure ....................................................................284
Potential Impact ....................................................................284

Enable Safe DLL Search Order: Enable Safe DLL search mode
(recommended) .......................................................................285
Vulnerability .........................................................................285
Countermeasure ....................................................................285
Potential Impact ....................................................................285

Make Screensaver Password Protection Immediate: The time in seconds
before the screen saver grace period expires (0 recommended) ........286
Vulnerability .........................................................................286
Countermeasure ....................................................................286
Potential Impact ....................................................................286

Security Log Near Capacity Warning: Percentage threshold for the security
event log at which the system will generate a warning .................287
Vulnerability .........................................................................287
Countermeasure ....................................................................287
Potential Impact ....................................................................287

Registry Entries Available in Windows XP with SP2 and
Windows Server 2003 with SP1 .................................................288

RestrictRemoteClients ..........................................................288
Vulnerability .........................................................................288
Countermeasure ....................................................................288
Potential Impact ....................................................................289

EnableAuthEpResolution .........................................................289
Vulnerability .........................................................................289
Countermeasure ....................................................................289
Potential Impact ....................................................................289
<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Countermeasure</th>
<th>Potential Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>RunInvalidSignatures</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vulnerability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Countermeasure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Potential Impact</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Registry Entries Available in Windows XP with SP2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Center Registry Entries for XP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vulnerability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Countermeasure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Potential Impact</td>
<td></td>
<td></td>
</tr>
<tr>
<td>StorageDevicePolicies\WriteProtect</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vulnerability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Countermeasure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Potential Impact</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Registry Entries Available in Windows Server 2003 with SP1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UseBasicAuth</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vulnerability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Countermeasure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Potential Impact</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DisableBasicOverClearChannel</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vulnerability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Countermeasure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Potential Impact</td>
<td></td>
<td></td>
</tr>
<tr>
<td>More Information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Member Server Hardening Procedures</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Securing the Accounts</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vulnerability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Countermeasure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Potential Impact</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTFS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vulnerability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Countermeasure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Potential Impact</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data and Application Segmentation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vulnerability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Countermeasure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Potential Impact</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Feedback

The Microsoft Solutions for Security and Compliance team would appreciate your thoughts about this and other security solutions.


Or e-mail your feedback to the following address: secwish@microsoft.com.

We look forward to hearing from you.
Introduction to Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP

The purpose of this guide is to provide you with a reference to security settings that provide countermeasures for specific threats against current versions of the Microsoft® Windows® operating systems.

This guide is a companion for two other publications that are available from Microsoft:


Many of the countermeasures that are described in this guide are not intended for specific computer roles in the companion guides, or in some cases for any roles at all. These countermeasures help assure compatibility, usability, manageability, availability, or performance.

Although often stated, it is nonetheless worth repeating that security and functionality are the opposite extremes of a continuum; the greater the level of security, the lower the level of functionality, and vice versa. There are exceptions, and some security countermeasures actually help to improve functionality, but for the most part this adage holds true.

The chapter structure of this guide is similar to the way the major setting sections display in the user interface of the Group Policy Object Editor. Each chapter begins with a brief explanation of what is in the chapter, followed by a list of subsection headers, each of which corresponds to a setting or group of settings. (These settings are listed in the Microsoft Excel® workbook that is described later in this chapter.) Each subsection includes a brief explanation of what the countermeasure does, and includes the following three additional subsections:

- **Vulnerability.** Explains how an attacker might exploit a feature or its configuration.
- **Countermeasure.** Explains how to implement the countermeasure.
- **Potential Impact.** Explains the possible negative consequences of countermeasure implementation.
For example, Chapter 2, "Domain Level Policies," begins with the following sections:

**Account Policies**

- Enforce password history
  - Vulnerability
  - Countermeasure
  - Potential Impact
- Maximum Password Age
  - Vulnerability
  - Countermeasure
  - Potential Impact

This pattern is repeated throughout this guide. Settings that are closely related are presented in a single section. For example, in Chapter 5, "Security Options," four settings are all placed into the "Microsoft network client and server: Digitally sign communications (four related settings)" section. These settings include the following:

- Microsoft Network Client: Digitally Sign Communications (Always)
- Microsoft Network Server: Digitally Sign Communications (Always)
- Microsoft Network Client: Digitally Sign Communications (If Server Agrees)
- Microsoft Network Server: Digitally Sign Communications (If Client Agrees)

Although many Group Policy settings are documented in this guide, those that are intended to help organizations manage their environments are not documented. This guide only examines the settings and features in Microsoft Windows Server™ 2003 with SP1 and Windows XP with SP2 that can help organizations secure their enterprises against specific threats. Settings and features that were added subsequent to those Service Packs, or functionalities that may be added by software released after those Service Packs, are not discussed in this guide. Also, management features and those security features that are not configurable by administrators are not described in this guide.

The information that is provided within this guide should help you and your organization understand the countermeasures that are available in current versions of the Windows operating system, but for prescriptive guidance about what settings to use for specific scenarios please refer to the two companion guides:

- **Windows XP Security Guide**, available online at [http://go.microsoft.com/fwlink/?LinkId=14839](http://go.microsoft.com/fwlink/?LinkId=14839)

The Microsoft Excel workbook "Windows Default Security and Services Configuration" (included with this guide) documents the default settings. The first worksheet ("Windows Server 2003 Defaults") details all of the default Group Policy settings that are available in Windows Server 2003. This worksheet includes the following columns:

- The H column, **Policy Setting Name in User Interface**, is the name of the setting as it appears in the Windows Server 2003 Group Policy Editor snap-in.
- The J column, **Default Domain Policy**, is the value for that setting in the built-in Default Domain Policy that is created when you promote the first domain controller in a new Active Directory® directory service domain.
• The K column, **Default Domain Controller Policy**, is the value for that setting in the built-in Default Domain Controller Policy that is created when you promote the first domain controller in a new Active Directory domain.

• The L column, **Stand-Alone Server Default Settings**, is the default value for that setting on a stand-alone Windows Server 2003 computer.

• The M column, **Domain Controller Effective Default Settings**, indicates the effective value for a domain controller with the default settings still in place.

• The N column, **Member Server Effective Default Settings**, shows the effective value for a domain member with the default settings still in place.

"Effective Default Setting" means the actual setting that is in effect on the system if no security settings have been changed. The effective setting on a system is determined by the Group Policy engine when it processes Group Policy during the computer's startup. The engine assigns setting precedence as described in the "Group Policy Application" section of Chapter 2, "Windows Server 2003 Hardening Mechanisms" in the Windows Server 2003 Security Guide.

To make the spreadsheets easier to read, additional columns were inserted to illustrate the hierarchy of objects within the Group Policy Editor. Columns A through G represent one level each of the hierarchy. For example, **Computer Configuration** appears in column A, and **Security Settings** appears in column C. Column I was also inserted to make the spreadsheets easier to read.

The second worksheet ("Windows Server 2003 System Services") lists all of the services that are available in Windows Server 2003. This worksheet includes the following columns:

• The A column, **Full Service Name**, lists the services by their names as they appear in the graphical management tools such as the Microsoft Management Console (MMC) Services Manager extension.

• The B column, **Service Name**, lists the services by their short name, which is the format used by many command-line tools.

• The C column, **DC Startup Type**, shows the default startup state for the service on a Windows Server 2003 domain controller.

• The D column, **Member Server Startup Type**, shows the default startup state for the service on a Windows Server 2003 computer that is a member of an Active Directory–based domain.

• The E column, **Stand-Alone Server Startup Type**, shows the default startup state for the service on a Windows Server 2003 stand-alone computer.

• The H column, **Logon As**, shows the account that the service uses to log on in a default configuration.

The format of the additional worksheets ("Windows XP Defaults" and "Windows XP System Services") is similar to these two worksheets. They provide information about the security settings and services in Windows XP.
Chapter Summaries

Windows Server 2003 with SP1 and Windows XP with SP2 provide the most dependable versions of these operating systems to date, with improved security and privacy features. This guide consists of twelve chapters, and chapters 2 through 6 discuss the procedures that help create a secure environment. Each chapter builds on an end-to-end process that helps secure computers that run these operating systems.

Chapter 1: Introduction to Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP

This chapter includes an overview of the guide, descriptions of the intended audience, the problems that are discussed in the guide, and the overall intent of the guide.

Chapter 2: Domain Level Policies

This chapter discusses the Group Policy settings that are applied at the domain level: password policies, account lockout policies, and Kerberos authentication protocol policies. Collectively, these policies are referred to as Account policies.

Chapter 3: Audit Policy

This chapter discusses the use of Audit policies to monitor and enforce your security measures. It describes the various settings and provides examples of how audit information is modified when the settings are changed.

Chapter 4: User Rights

This chapter discusses the various logon rights and privileges that are provided by the Windows operating systems, and provides guidance about which accounts should be assigned these rights.

Chapter 5: Security Options

This chapter introduces the "Security Options" section of Group Policy and provides guidance about security settings for digital data signatures, Administrator and Guest account names, access to floppy disk and CD-ROM drives, driver installation behavior, and logon prompts.

Chapter 6: Event Log

This chapter provides guidance about how to configure the settings that relate to the various event logs on Windows Server 2003 and Windows XP computers.

Chapter 7: System Services

Windows XP and Windows Server 2003 include a variety of system services. Many of these services are configured to run by default, but others are not present unless you install specific components. This chapter lists the various services that come with the
operating systems and provides specific recommendations about which ones to leave enabled and which ones can be safely disabled.

Chapter 8: Software Restriction Policies

This chapter provides a brief overview of the software restriction policy mechanism, which was introduced in Windows XP and Windows Server 2003. It provides links to additional resources about how to design and use software restriction policies.

Chapter 9: Windows XP and Windows Server 2003 Administrative Templates

This chapter lists the settings that are available through the Group Policy Administrative Templates. It does not examine every available setting, but focuses on those settings that relate to security.

Chapter 10: Additional Registry Entries

This chapter provides information about additional registry entries that are not listed in the Administrative Template file, but are present in the baseline security template. It provides instructions about how to modify the interface of the Security Configuration Editor to expose these entries in the user interface. It also provides additional registry entries that are available in Windows XP SP2 and Windows Server 2003 SP1.

Chapter 11: Additional Countermeasures

This chapter describes a number of additional security measures that may need to be applied to your computers. However, these countermeasures cannot be easily applied through Group Policy or other automated means. These countermeasures include securing accounts on member servers, NTFS settings, data and application segmentation, SNMP community name settings, disabling NetBIOS bindings, Terminal Services configuration, Dr. Watson, IPsec policies, and a pointer to more extensive guidance on the Windows Firewall.

Chapter 12: Conclusion

The final chapter reviews the important points of the guide in a brief overview of everything that was discussed in the previous chapters.
Tools and Templates

A collection of files is included with the downloadable version of this guide to help your organization to evaluate, test, and implement the recommended countermeasures. These files are collectively referred to as tools and templates.

The files are included in a .msi file within the self-extracting WinZip archive that contains this guide, which is available on the Microsoft Download Center at http://go.microsoft.com/fwlink/?LinkId=15160. When you execute the .msi file, the following folder structure will be created in the location you specify:

- The \Threats and Countermeasures Guide Tools and Templates folder contains the Microsoft Excel workbook "Windows Default Security and Services Configuration.xls," which summarizes the service and default settings for Windows Server 2003 with SP1 and Windows XP with SP2.

- The \Threats and Countermeasures Guide Tools and Templates\SCE Update folder includes text files and script files. You can use the text files to modify and customize the user interface of the Security Configuration Editor. You can use the script files to automatically apply these settings or roll them back. These procedures are detailed in Chapter 10, "Additional Registry Entries."
Domain Level Policies

This chapter discusses those Group Policy settings that are applied at the domain level. The built-in Default Domain Controller policy includes default setting values for these policies, which are collectively referred to as Account policies.

Account Policies

There are three different types of Account policies: password policies, account lockout policies, and Kerberos authentication protocol policies. A single Microsoft Windows Server™ 2003 domain may have one of each of these policies. If these policies are set at any other level in Active Directory, only local accounts on member servers will be affected.

Note: For domain accounts, there can be only one Account policy per domain. The Account policy must be defined in the Default Domain Policy or in a new policy that is linked to the root of the domain and given precedence over the Default Domain Policy, which is enforced by the domain controllers that make up the domain. A domain controller always pulls the Account policy from the root of the domain, even if there is a different Account policy applied to the OU that contains the domain controller. The root of the domain is the top level container of the domain, not to be confused with the root domain in a forest; the root domain in a forest is the top level domain within that forest.

The Account policy settings in Group Policy are all applied at the domain level. Default values are present in the built-in Default Domain Controller policy for password policies, account lockout policies, and Kerberos policies. When you configure these policies in the Active Directory® directory service, remember that Microsoft® Windows® only allows one domain Account policy—the Account policy that is applied to the root domain of the domain tree. The domain Account policy will become the default Account policy of any Windows computer that is a member of the domain.

The only exception to this rule is when another Account policy is defined for an organizational unit (OU). The Account policy settings for the OU will affect the local policy on any computers that are contained in the OU. For example, if an OU policy defines a maximum password age that differs from the domain-level Account policy, the OU policy will only be applied and enforced when users log on to the local computer. Only default local computer policies will apply to computers that are in a workgroup or in a domain where neither an OU Account policy nor a domain policy applies.

The settings for each of these policy types are discussed throughout this chapter.
Password Policy

In Windows and many other operating systems, the most common method to authenticate a user's identity is to use a secret pass phrase or password. A secure network environment requires all users to use strong passwords (ones that have at least ten characters and include a combination of letters, numbers, and symbols). These passwords help prevent the compromise of user accounts and administrative accounts by unauthorized people who use either manual methods or automated tools to guess weak passwords. Strong passwords that are changed regularly reduce the likelihood of a successful password attack. (More detailed information about strong passwords is provided in the "Passwords must meet complexity requirements" section later in this chapter.)

You can enforce the use of strong passwords through an appropriate password policy. Password policy settings control the complexity and lifetime of passwords. This section discusses each specific password policy account setting. This guide also includes a Microsoft Excel® workbook, "Windows Default Security and Services Configuration," that documents the default settings.

You can configure the password policy settings in the following location within the Group Policy Object Editor:

\Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy

If groups exist that require separate password policies, they should be segmented into another domain or forest based on any additional requirements.

Enforce password history

This policy setting determines the number of unique new passwords that must be associated with a user account before an old password can be reused.

The possible values for the Enforce password history setting are:

- A user-specified value between 0 and 24
- Not Defined

Vulnerability

Password reuse is an important concern in any organization. Many users will want to use or reuse the same password for their account over a long period of time. The longer the same password is in use for a particular account, the greater the chance that an attacker will be able to determine the password through brute-force attacks. Also, any accounts that may have been compromised will remain exploitable for as long as the password is left unchanged. If password changes are required but password reuse is not prevented, or if users can continually reuse a small number of passwords, the effectiveness of a good password policy is greatly reduced.

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

Countermeasure

Configure the Enforce password history setting to 24, the maximum setting, to help minimize the number of vulnerabilities that are caused by password reuse.
For this setting to be effective in your organization, do not allow passwords to be changed immediately when you configure the **Minimum password age** setting. The **Enforce password history** value should be set at a level that combines a reasonable maximum password age with a reasonable password change interval requirement for all users in your organization.

**Potential Impact**

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

This policy setting determines the number of days that a password can be used before the user must change it.

The possible values for the Maximum password age setting are:

- A user-specified number of days between 0 and 999
- Not Defined

Vulnerability

Any password, even the most complex password, can be guessed (or "cracked") by an attacker with sufficient time and computer processing power. Some of the following policy settings can make it harder to crack passwords in a reasonable amount of time. The risk of a valid password being cracked can be reduced if users are frequently required to change their passwords, which can also mitigate the risk of unauthorized logon by someone who wrongfully acquired a password. You can configure the Maximum password age setting so that users are never required to change their passwords, but such a configuration would be a major security risk.

Countermeasure

Configure the Maximum password age setting to a value that is suitable for your organization’s business requirements. Microsoft recommends a value of 90 days for most organizations. Although such a configuration is not recommended, you can configure the Maximum Password Age setting to 0 so that passwords will never expire.

Potential Impact

If the Maximum password age setting is too low, users will be required to change their passwords very often. Such a configuration may actually reduce security in the organization, because users may be more likely to write their passwords somewhere so that they do not forget them and then leave the information in an insecure location or lose it. If you configure the value for this policy setting too high, the level of security within an organization will be reduced because it will allow potential attackers a much larger timeframe in which to crack user passwords or to use compromised accounts.

Minimum password age

This policy setting determines the number of days that a password must be used before the user is allowed to change it. The Minimum password age value must be less than the Maximum password age value.

Configure this policy setting to a number that is greater than 0 if you want the Enforce password history setting to be effective. If you configure the Enforce password history setting to 0, the user is not required to choose a new unique password when they are prompted to change their password. If password history is used, users will have to enter a new unique password when they change their password.

The possible values for the Minimum password age setting are:

- A user-specified number of days between 0 and 998
- Not Defined
Vulnerability

It is ineffective to require users to change passwords regularly if they can cycle through passwords until they can reuse a favorite password. Use this policy setting with the Enforce password history setting to prevent the reuse of old passwords. For example, if you configure the Enforce password history setting to ensure that users cannot reuse any of their last 12 passwords, they could change their password 13 times in a few minutes and reuse the password they started with unless you configure the Minimum password age setting to a number that is greater than 0. You must configure this policy setting to a number that is greater than 0 for the Enforce password history setting to be effective.

Countermeasure

Configure the Minimum password age setting to a value of at least 2 days. If you configure the number of days to 0, immediate password changes would be allowed, which is not recommended.

Potential Impact

One minor issue is associated with a Minimum password age setting configuration of a number that is greater than 0. If an administrator sets a password for a user but would like that user to change the password when they first log on, the administrator must select the User must change password at next logon check box. Otherwise, the user will not be able to change the password until the next day.

Minimum password length

This policy setting determines the least number of characters that may make up a password for a user account. There are many different theories about how to determine the best password length for an organization, but perhaps "pass phrase" is a better term than "password." In Microsoft Windows 2000 and later versions, pass phrases can be quite long and they can include spaces, punctuation marks, and Unicode characters. Therefore, a phrase such as "I want to drink a $5 beverage!" is a valid pass phrase. Such a phrase is considerably stronger than an 8 or 10 character string of random numbers and letters, but it is easier to remember.

The possible values for the Minimum password length setting are:

- A user-specified number between 0 and 14
- Not Defined

Vulnerability

There are several types of password attacks that can be performed to obtain the password for a particular user account. These attacks include dictionary attacks (which attempt to use common words and phrases) and brute force attacks (which try every possible combination of characters). Also, attackers sometimes try to obtain the account database so they can use utilities to crack the accounts and passwords.

Countermeasure

Configure the Minimum password length setting to a value of 8 or more. If the number of characters is set to 0, no password will be required.

In most environments, an 8-character password is recommended because it is long enough to provide adequate security but not too difficult for users to easily remember. This configuration will provide adequate defense against a brute force attack. Additional
complexity requirements will help reduce the possibility of a dictionary attack. Complexity requirements are discussed in the next section of this chapter. You should also note that some countries have legal requirements with respect to password length.

**Potential Impact**

Requirements for extremely long passwords can actually decrease the security of an organization, because users may be more likely to write their passwords somewhere so that they do not forget them and then leave the information in an insecure location or lose it. However, if users are taught that they can use pass phrases as described earlier, they should be able to easily remember them.

If short passwords are permitted, security will be reduced because they can be easily cracked with tools that perform either dictionary or brute force attacks. If very long passwords are required, mistyped passwords could cause account lockouts and subsequently increase the volume of help desk calls.

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

**Passwords must meet complexity requirements**

This policy setting determines whether passwords must meet a series of guidelines that are considered important for a strong password.

If this policy setting is enabled, passwords must meet the following requirements:

- The password is at least six characters long.
- The password contains characters from three of the following four categories:
  - Uppercase characters (A, B, C, …)
  - Lowercase characters (a, b, c, …)
  - Numerals (0, 1, 2, 3, 4, 5, 6, 7, 8, 9)
  - Non-alphanumeric and Unicode characters (( ) ` ~ ! @ # $ % ^ & * - + = | \ { } [ ] : ; " ' < > , . ? / € Γ ƒ λ and space)
- The password does not contain three or more consecutive characters from the user's account name or display name. If the account name is less than three characters long, then this check is not performed because the rate at which passwords would be rejected would be too high. When a check is performed against the user's full name, several characters are treated as delimiters that separate the name into individual tokens: commas, periods, dashes/hyphens, underscores, spaces, pound signs and tabs. For each token that is three or more characters long, that token is searched for in the password and if it is present the password change is rejected.

For example, the name Erin M. Hagens would be split into three tokens: Erin, M, and Hagens. Because the second token is only one character long it would be ignored. Therefore this user could not have a password that included either "erin" or "hagens" as a substring anywhere in the password. All of these checks are case insensitive.

These complexity requirements are enforced upon password change or creation of new passwords.

The rules that are included in the Windows Server 2003 policy cannot be directly modified. However, you can create a new version of the Passfilt.dll file to apply a different set of rules. For more information about how to create your own password filter, see the Password Filters documentation in the Windows Platform software development kit.
The possible values for the **Passwords must meet complexity requirements** setting are:

- Enabled
- Disabled
- Not Defined

**Vulnerability**

Passwords that contain only alphanumerical characters are extremely easy to crack with several publicly available utilities. To prevent passwords from being cracked, they should contain a wider range of characters.

**Countermeasure**

Configure the **Passwords must meet complexity requirements** setting to **Enabled**.

When combined with a **Minimum password length** of 8, this policy setting ensures that the number of different possibilities for a single password is so great that it will be difficult (but not impossible) for a brute force attack to succeed. An attacker who had enough processing power to test 1 million passwords per second could determine such a password in about seven and one-half days or less. (If the **Minimum password length** setting is increased, the average amount of time necessary for a successful attack will also increase.)

**Potential Impact**

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

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

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

**Store password using reversible encryption for all users in the domain**

Threats and Countermeasures

The Store password using reversible encryption for all users in the domain setting provides support for application protocols that require knowledge of the user’s password for authentication purposes. However, encrypted passwords that are stored in a way that is reversible can be decrypted. A knowledgeable attacker who was able to break this encryption could then log on to network resources with the compromised account.

Caution: Never enable this policy setting unless business requirements outweigh the need to protect password information.

Use of Challenge Handshake Authentication Protocol (CHAP) authentication through remote access or Internet Authentication Service (IAS) services requires that this policy setting be enabled. CHAP is an authentication protocol that can be used by Microsoft remote access and Network Connections.

The possible values for the Store password using reversible encryption for all users in the domain setting are:

- Enabled
- Disabled
- Not Defined

Vulnerability

This policy setting determines whether Windows Server 2003 will store passwords in a weaker format that is much more susceptible to compromise.

Countermeasure

Configure the Store password using reversible encryption for all users in the domain setting to Disabled.

Potential Impact

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

Account Lockout Policy

More than a few unsuccessful password submissions during an attempt to log on to a computer might represent an attacker’s attempts to determine an account password by trial and error. Windows Server 2003 with SP1 tracks logon attempts, and you can configure the operating system to disable the account for a preset period of time after a specified number of failed attempts. Account lockout policy settings control the threshold for this response and what action to take after the threshold is reached. This guide includes a Microsoft Excel workbook, "Windows Default Security and Services Configuration," that documents the default settings.

You can configure the account lockout policy settings in the following location within the Group Policy Object Editor:

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

This policy setting determines the number of minutes that a locked-out account remains locked out before it is automatically unlocked. The available range is from 1 to 99,999 minutes. To specify that the account will be locked out until an administrator manually unlocks it, configure the value to 0. If an account lockout threshold is defined, the Account lockout duration must be greater than or equal to the reset time.

The possible values for the Account lockout duration setting are:

- A user-defined value in minutes between 0 and 99,999
- Not Defined

Vulnerability

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

Countermeasure

Configure the Account lockout duration setting to an appropriate value for your environment. To specify that the account will remain locked until an administrator manually unlocks it, configure the value to 0. When the Account lockout duration setting is configured to a non-zero value, automated attempts to guess account passwords must wait out this interval before they resume attempts against a specific account. If you use this setting in combination with the Account lockout threshold setting, such automated password guessing attempts can be made difficult or useless.

Potential Impact

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

Account lockout threshold

This policy setting determines the number of failed logon attempts that causes a user account to become locked out. A locked-out account cannot be used until it is reset by an administrator or until the lockout duration for the account expires. You can specify up to 999 failed logon attempts, or you can set the value to 0 to specify that the account will never be locked out. If you define an Account lockout threshold, then the Account lockout duration must be greater than or equal to the reset time.

Failed password attempts against workstations or member servers that have been locked using either CTRL+ALT+DELETE or password-protected screen savers do not count as failed logon attempts unless the policy setting Interactive logon: Require Domain Controller authentication to unlock workstation is enabled. If it is, then repeated failed password attempts to unlock the workstation will count against the account lockout threshold.
The possible values for the **Account lockout threshold** setting are:

- A user-defined value between 0 and 999
- Not Defined

**Vulnerability**

Password attacks may use automated methods to try thousands or even millions of password combinations for any or all user accounts. The effectiveness of such attacks can be almost eliminated if you limit the number of failed logons that can be performed.

However, it is important to note that a DoS attack could be performed on a domain that has an account lockout threshold configured. A malicious attacker could programmatically attempt a series of password attacks against all users in the organization. If the number of attempts is greater than the account lockout threshold, the attacker may be able to lock out every account.

**Countermeasure**

Because vulnerabilities can exist when this value is configured as well as when it is not configured, two distinct countermeasures are defined. Any organization should weigh the choice between the two based on their identified threats and the risks that they wish to mitigate. The two countermeasure options are:

- Configure the **Account Lockout Threshold** setting to 0. This configuration ensures that accounts will not be locked out, and will prevent a DoS attack that intentionally attempts to lock out all, or some specific, accounts. This configuration also helps reduce help desk calls because users cannot accidentally lock themselves out of their accounts.

  Because it will not prevent a brute force attack, this configuration should only be chosen if both of the following criteria are explicitly met:
  - The password policy requires all users to have complex passwords of 8 or more characters.
  - A robust audit mechanism is in place to alert administrators when a series of failed logons occur in the environment.

- If your organization cannot meet the previous criteria, configure the **Account Lockout Threshold** setting to a sufficiently high value that will provide users with the ability to accidentally mistype their password several times before the account is locked, but ensure that a brute force password attack will still lock the account. A good recommendation for such a configuration is 50 invalid logon attempts, which will prevent accidental account lockouts and reduce the number of help desk calls but will not prevent a DoS attack (as discussed earlier).

**Potential Impact**

If this policy setting is enabled, a locked-out account will not be usable until it is reset by an administrator or until the account lockout duration expires. This setting will likely generate a number of additional help desk calls. In fact, locked accounts cause the greatest number of calls to the help desk in many organizations.

If you configure the **Account Lockout Threshold** to 0, there is a possibility that an attacker's attempt to crack passwords with a brute force password attack may go undetected if a robust audit mechanism is not in place.
Reset account lockout counter after

This policy setting determines the number of minutes that must elapse before the counter that tracks failed logon attempts and triggers account lockouts is reset to 0. If an Account lockout threshold is defined, this reset time must be less than or equal to the Account lockout duration setting configuration.

The possible values for the Reset account lockout counter after setting are:

- A user-defined number of minutes between 1 and 99,999
- Not Defined

**Vulnerability**

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

**Countermeasure**

Configure the Reset account lockout counter after setting to 30 minutes.

**Potential Impact**

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

In Windows Server 2003 with SP1, the Kerberos authentication protocol provides the default mechanism for domain authentication services and the authorization data that is necessary for a user to access a resource and perform a task on that resource. If the lifetime of Kerberos tickets is reduced, the risk of a legitimate user's credentials being stolen and successfully used by an attacker decreases. However, authorization overhead increases.

In most environments, the Kerberos policy settings should not need to be changed. These policy settings are applied at the domain level, and the default values are configured in the Default Domain Policy GPO in a default installation of a Windows 2000 or Windows Server 2003 Active Directory domain. This guide includes a Microsoft Excel workbook, "Windows Default Security and Services Configuration," that documents the default settings.

You can configure the Kerberos policy settings in the following location within the Group Policy Object Editor:

```
Computer Configuration\Windows Settings\Security Settings\Account Policies\Kerberos Policy
```

**Enforce user logon restrictions**

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

The possible values for the Enforce user logon restrictions setting are:

- Enabled
- Disabled
- Not Defined

**Vulnerability**

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.

**Countermeasure**

Configure the Enforce user logon restrictions setting to Enabled.

**Potential Impact**

None. This is the default configuration.

**Maximum lifetime for service ticket**

This policy 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 10 minutes or greater, and less than or equal to the configuration of the Maximum lifetime for user ticket setting.

If a client presents an expired session ticket when it requests a connection to a server, the server returns an error message and the client must request a new session ticket from the KDC. After a connection is authenticated, however, it does not matter if the
session ticket remains valid. Session tickets are used only to authenticate new connections with servers. Operations are not interrupted if the session ticket that authenticated the connection expires during the connection.

The possible values for the **Maximum lifetime for service ticket** setting are:

- A user-defined value in minutes between 10 and 99,999. If you configure this policy setting to 0, service tickets do not expire.
- Not Defined.

**Vulnerability**

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.

**Countermeasure**

Configure the **Maximum lifetime for service ticket** setting to **600 minutes**.

**Potential Impact**

None. This is the default configuration.

**Maximum lifetime for user ticket**

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

The possible values for the **Maximum lifetime for user ticket** setting are:

- A user-defined value in hours between 0 and 99,999. The default value is 10 hours.
- Not Defined.

**Vulnerability**

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.

**Countermeasure**

Configure the **Maximum lifetime for user ticket** setting to **10 hours**.

**Potential Impact**

None. This is the default configuration.

**Maximum lifetime for user ticket renewal**

This policy setting determines the period of time (in days) during which a user's ticket-granting ticket (TGT) may be renewed.
The possible values for the **Maximum lifetime for user ticket renewal** setting are:

- A user-defined value in minutes between 0 and 99,999
- Not Defined

**Vulnerability**

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

**Countermeasure**

Configure the **Maximum lifetime for user ticket renewal** setting to **10080 minutes** (7 days).

**Potential Impact**

None. This is the default configuration.

---

**Maximum tolerance for computer clock synchronization**

This policy setting determines the maximum time difference (in minutes) that the Kerberos protocol will allow between the time on the client computer's clock and the time on the Windows Server 2003–based domain controller that provides Kerberos authentication.

The possible values for the **Maximum tolerance for computer clock synchronization** setting are:

- A user-defined value in minutes between 1 and 99,999
- Not Defined

**Vulnerability**

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.

**Countermeasure**

Configure the **Maximum tolerance for computer clock synchronization** setting to **5 minutes**.

**Potential Impact**

None. This is the default configuration.
More Information

The following links provide additional information about topics that relate to hardening domain controllers that run Windows Server 2003 with SP1:

• For a detailed explanation of how password complexity works in Windows as well as specific advice on how to create stronger passwords that are not too difficult to remember, see the article "Selecting Secure Passwords," which is available online at www.microsoft.com/smallbusiness/support/articles/select_sec_passwords.mspx.


• For more information about Group Policies, including a listing of paths and values for all settings that are stored in the registry and under which are available for each version of Windows each is available, see “Group Policy Settings Reference for Windows Server 2003 with Service Pack 1” at www.microsoft.com/downloads/details.aspx?FamilyId=7821C32F-DA15-438D-8E48-45915CD2BC14.
Audit Policy

An audit log records an entry whenever users perform certain specified actions. For example, the modification of a file or a policy can trigger an audit entry that shows the action that was performed, the associated user account, and the date and time of the action. You can audit both successful and failed attempts at actions.

The state of the operating system and applications on a computer is dynamic. For example, security levels may be temporarily changed to enable immediate resolution of an administration or network issue. However, such changes are often forgotten about and never undone. If security levels are not properly reset, a computer may no longer meet the requirements for enterprise security.

Regular security analyses enable administrators to track and determine that adequate security measures are in effect for each computer as part of an enterprise risk management program. Such analyses focus on highly specific information about all aspects of a computer that relate to security, which administrators can use to adjust the security levels. More importantly, this information can help detect any security flaws that may occur in the computer over time.

Security audits are extremely important for any enterprise network, because audit logs may provide the only indication that a security breach has occurred. If the breach is discovered some other way, proper audit settings will generate an audit log that contains important information about the breach.

Oftentimes, failure logs are much more informative than success logs because failures typically indicate errors. For example, successful logon to a computer by a user would typically be considered normal. However, if someone unsuccessfully tries to log on to a computer multiple times, it may indicate an attacker's attempt to break into the computer with someone else's account credentials. The event logs record events on the computer, and in Microsoft® Windows® operating systems, there are separate event logs for applications, security events, and system events. The Security log records audit events. The event log container of Group Policy is used to define attributes that relate to the Application, Security, and System event logs, such as maximum log size, access rights for each log, and retention settings and methods. This guide includes a Microsoft Excel® workbook, "Windows Default Security and Services Configuration," that documents the default settings.

Before any audit processes are implemented, an organization should determine how they will collect, organize, and analyze the data. There is little value in large volumes of audit data if there is no underlying plan to exploit it. Also, audit settings can affect computer performance. The effect of a given combination of settings may be negligible on an end-user computer but quite noticeable on a busy server. Therefore, you should perform
some performance tests before you deploy new audit settings in your production environment.

You can configure the Audit policy settings in the following location within the Group Policy Object Editor:

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

The vulnerabilities, countermeasures, and potential impacts of all the audit settings are identical. Therefore, these terms are described only once. Each description is then followed by brief explanations of each setting.

The options for each of the audit settings are:

• **Success.** An audit entry is generated when the requested action succeeds.

• **Failure.** An audit entry is generated when the requested action fails.

• **No Auditing.** No audit entry is generated for the associated action.

Vulnerability

If no audit settings are configured, it will be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that too many authorized activities generate events, the Security event log will be filled with useless data. Also, you can affect overall computer performance if you configure audit settings for a large number of objects.

Countermeasure

You should enable sensible Audit policy settings for all computers in your organization so that users can be held accountable for their actions and unauthorized activity can be detected and tracked.

Potential Impact

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, 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 may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit account logon events

This policy setting determines whether to audit each instance of user logon or logoff on a different computer than the one that records the event and validates the account. If you configure this policy setting, you can specify whether to audit successes, audit failures, or not audit the event type at all. Success audits generate an audit entry when an account logon attempt succeeds, which is useful information for accounting purposes and for post-incident forensics so that you can determine who successfully logged into which computer. Failure audits generate an audit entry when an account logon attempt fails, which is useful for intrusion detection. However, this policy setting also creates the potential for a denial of service (DoS) attack. When the **Audit: Shut down system immediately if unable to log security audits** setting is enabled, an attacker could generate millions of logon failures, fill the Security event log, and force the computer to shut down.

If you configure the **Audit account logon events** setting to **Success** on a domain controller, an entry is logged for each user who is validated against that domain controller, even though the user actually logs on to a workstation or server that is joined to the domain.
Audit account management

This policy setting determines whether to audit each account management event on a computer. Examples of account management events include the following:

- A user account or group is created, changed, or deleted.
- A user account is renamed, disabled, or enabled.
- A password is set or changed.

If you configure the Audit account management setting, you can specify whether to audit successes, audit failures, or not audit the event type at all. Success audits generate an audit entry when any account management event succeeds, and you should enable them on all computers in your enterprise. When an organization responds to security incidents, it is critical that they be able to track who created, changed, or deleted an account. Failure audits generate an audit entry when any account management event fails.

Audit directory service access

This policy setting determines whether to audit user access of an Active Directory® directory service object that has an associated system access control list (SACL). A SACL is list of users and groups for which actions on an object are to be audited on a Microsoft Windows–based network.

If you configure the Audit directory service access setting, you can specify whether to audit successes, audit 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 SACL that indicates that the user should be audited for the requested action. Failure audits generate an audit entry when a user unsuccessfully attempts to access an Active Directory object that has a SACL that requires auditing. (Both types of audit entries are created before the user is notified that the request succeeded or failed.) If you enable this policy setting 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 these settings if you actually intend to use the information that is created.

Note: You can configure a SACL on an Active Directory object through the Security tab in that object's Properties dialog box. This method is analogous to Audit object access, except that it applies only to Active Directory objects and not to file system and registry objects.

Audit logon events

This policy setting determines whether to audit each instance of user logon, logoff, or network connection to the computer that records the audit event. If you log successful account logon audit events on a domain controller, workstation logon attempts do not generate logon audits. Only interactive and network logon attempts to the domain controller itself generate logon events on the domain controller. To summarize, account logon events are generated where the account lives, and logon events are generated where the logon attempt occurs.

If you configure the Audit logon events setting, you can specify whether to audit successes, audit failures, or not audit the event type at all. Success audits generate an audit entry when a logon attempt succeeds, which is useful information for accounting purposes and for post-incident forensics so that you can determine who successfully logged on to which computer. Failure audits generate an audit entry when a logon attempt fails, which is useful for intrusion detection. However, this configuration also creates a potential DoS condition, because an attacker could generate millions of logon failures, fill the Security event log, and force the server to shut down.
**Audit object access**

This policy setting determines whether to audit the event of a user who accesses an object—for example, a file, folder, registry key, or printer—that has a SACL that specifies a requirement for auditing.

If you configure the **Audit object access** setting, you can specify whether to audit successes, audit failures, or not audit the event type at all. Success audits generate an audit entry when a user successfully accesses an object that has a SACL. Failure audits generate an audit entry when a user unsuccessfully attempts to access an object that has a SACL (some failure events are to be expected during normal computer operations). For example, many applications (such as Microsoft Word) always attempt to open files with both read and write privileges. If the applications are unable to do so, they then try to open the files with read-only privileges. If you enable failure auditing and the appropriate SACL on the file, a failure event will be recorded when such an event occurs.

In Microsoft Windows Server™ 2003 with Service Pack 1 (SP1), you can audit access to objects that are stored in the Internet Information server (IIS) metabase. To enable metabase object auditing, you must enable **Audit object access** on the target computer, and then set SACLs on the specific metabase objects whose access you want to audit.

If you configure the **Audit object access** policy setting and configure SACLs on objects, a large volume of entries can be generated in the Security logs on computers in your organization. Therefore, you should only enable these settings if you actually intend to use the information that is logged.

**Note:** You must perform a two-step process to enable the capability to audit an object, such as a file, folder, printer, or registry key, in Windows Server 2003. After you enable the audit object access policy, you must determine the objects whose access you want to monitor, and then modify their SACLs accordingly. For example, if you want to audit any attempts by users to open a particular file, you can configure a Success or Failure audit attribute directly on the file that you want to monitor for that particular event with Windows Explorer or Group Policy.

**Audit policy change**

This policy setting determines whether to audit every incidence of a change to user rights assignment policies, Windows Firewall policies, Audit policies, or trust policies.

If you configure the **Audit policy change** setting, you can specify whether to audit successes, audit failures, or not audit the event type at all. Success audits generate an audit entry when a change to user rights assignment policies, Audit policies, or trust policies is successful. This audit information is useful for accounting purposes and can help you determine who successfully modified policies in the domain or on individual computers. Failure audits generate an audit entry when a change to user rights assignment policies, Audit policies, or trust policies fails.

If you enable the **Audit policy change** setting in Windows XP with SP2 and Windows Server 2003 with SP1, logging of configuration changes for the Windows Firewall component is also enabled.

**Audit privilege use**

This policy setting determines whether to audit each instance of a user who exercises a user right.

If you configure the **Audit privilege use** setting, you can specify whether to audit successes, audit failures, or not audit the event type at all. Success audits generate an audit entry when the exercise of a user right succeeds. Failure audits generate an audit entry when the exercise of a user right fails. If you enable this policy setting, the volume
of events that is generated can be very large and the events may be difficult to sort through. You should only enable this setting if you have a plan for how you will use the information that is generated.

Audit events are not generated for use of the following user rights, even if success audits or failure audits are specified for this policy setting:

- Bypass traverse checking
- Debug programs
- Create a token object
- Replace process level token
- Generate security audits
- Backup files and directories
- Restore files and directories
Audit process tracking

This policy setting determines whether to audit detailed tracking information for events such as program activation, process exit, handle duplication, and indirect object access.

If you configure the Audit process tracking setting, you can specify whether to audit successes, audit failures, or not audit the event type at all. Success audits generate an audit entry when the process being tracked succeeds. Failure audits generate an audit entry when the process being tracked fails.

If you enable Audit process tracking in Windows XP with SP2 and Windows Server 2003 with SP1, Windows will also log information about the operating mode and status of the Windows Firewall component.

When enabled, the Audit process tracking setting generates a large number of events. This policy setting is typically configured to No Auditing. However, the information that this policy setting generates can be very beneficial during an incident response because it provides a detailed log of the processes that were started and when they were launched.

Audit system events

This policy setting determines whether to audit when a user restarts or shuts down their computer, or when an event occurs that affects either computer security or the Security log.

If you configure the Audit system events setting, you can specify whether to audit successes, audit failures, or not audit the event type at all. Success audits generate an audit entry when an event executes successfully. Failure audits generate an audit entry when an event is unsuccessful. Because few additional events are recorded if both failure and success audits are enabled for system events, and because all such events are very significant, you should configure this policy setting to Enabled on all computers in your organization.
Audit Example: Results of a User Logon Event

After you become familiar with the different audit settings that are available in Windows, it may be helpful to consider a specific example. Audits are performed from an individual computer's perspective, rather than from the more holistic perspective that an enterprise administrator may prefer. Because events are recorded on individual computers, you may need to examine the Security logs of multiple computers and correlate the data to determine what occurred.

The rest of this chapter shows the core events that are written to the event logs of a domain controller, a file server, and an end-user computer when an authorized user logs on to their computer and accesses a file on a shared folder that is hosted by the file server. Only the core events are documented—other events that are generated by these activities were omitted for the sake of clarity. The names of the accounts and resources involved in this example are:

• Domain = DOM
• Domain controller = DC1
• File server = FS1
• End-user computer = XP1
• User = John
• Shared folder on FS1 = Share
• Document in the shared folder = document.txt

**User logs on to their computer**

- Events recorded on the end user computer
  - Success Audit for Event ID 528, user Logon/Logoff for user DOM\John at computer XP1.

- Events recorded on the domain controller
  - Success Audit for Event ID 540, user Logon/Logoff for user DOM\John at computer DC1.

- Events recorded on the file server
  - Not applicable.

**User connects to the shared folder called Share**

- Events recorded on the end user computer
  - Not applicable.

- Events recorded on the domain controller
  - Success Audit for Event ID 673, Account logon for user John@DOM.com for service name FS1$.
  - Success Audit for Event ID 673, Account logon for user FS$@DOM.com for service name FS1$.
Chapter 3: Audit Policy

- Success Audit for Event ID 673, Account logon for user XP1$@DOM.com for service name FS1$.

  **Note:** These are all Kerberos authentication protocol service ticket requests.

- **Events recorded on the file server**
  - Success Audit for Event ID 540, user Logon/Logoff for user DOM\John at computer FS1.
  - Success Audit for Event ID 560, Object Access for user DOM\John to the object named C:\Share with access types READ_CONTROL, ReadData (or ListDirectory), ReadEA, and ReadAttributes.
  - Success Audit for Event ID 560, Object Access for user DOM\John to the object named C:\Share\document.txt with access types READ_CONTROL, ReadData (or ListDirectory), ReadEA, and ReadAttributes.

**User opens the file document.txt**

- **Events recorded on the end user computer**
  - Not applicable.

- **Events recorded on the domain controller**
  - Not applicable.

- **Events recorded on the file server**
  - Success Audit for Event ID 560, Object Access for user DOM\John to the object named C:\Share\document.txt with access types READ_CONTROL, ReadData (or ListDirectory), WriteDate (or AddFile), AppendDate (or AddSubdirectory or CreatePipeInstance), ReadEA, WriteEA, ReadAttributes, and WriteAttributes.
  - Success Audit for Event ID 560, Object Access for user DOM\John to the object named C:\Share\document.txt with access types ReadAttributes.
  - Success Audit for Event ID 560, Object Access for user DOM\John to the object named C:\Share with access types ReadAttributes.

**User saves the file document.txt**

- **Events recorded on the end user computer**
  - Not applicable.

- **Events recorded on the domain controller**
  - Not applicable.

- **Events recorded on the file server**
  - Success Audit for Event ID 560, Object Access for user DOM\John to the object named C:\Share\document.txt with access types SYNCHRONIZE, ReadData (or ListDirectory), WriteDate (or AddFile), AppendDate (or AddSubdirectory or CreatePipeInstance), ReadEA, WriteEA, ReadAttributes, and WriteAttributes.
  - Success Audit for Event ID 560, Object Access for user DOM\John to the object named C:\Share\document.txt with access types READ_CONTROL, SYNCHRONIZE and ReadData (or ListDirectory).

Although this example looks like a complex series of events, it has been greatly simplified. The listed actions would actually generate dozens of logon, logoff, and privilege use events on the domain controller and file server. When the user opens the file, scores of object access events are also generated, and each time the user saves the
file many more events are generated. As you can see, the use of audit data can be a challenge without the support of automated tools such as Microsoft Operations Manager.

**More Information**

The following links provide additional information about topics that relate to Audit policies for computers that run Windows XP with SP2 or Windows Server 2003 with SP1:

- For more Audit policy information, see the "Auditing Policy" section in the Windows Server 2003 TechCenter documentation on Microsoft TechNet at www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/6847e72b-9c47-42ab-b3e3-691addac9f33.mspx.

- The article "HOW TO: Use Group Policy to Audit Registry Keys in Windows Server 2003" at http://support.microsoft.com/default.aspx?kbid=324739 describes how to audit access to registry keys by adding SACLs to those keys.

User Rights

User rights allow users to perform tasks on a computer or a domain. User rights include logon rights and privileges. Logon rights control who is authorized to log on to a computer and how they can log on. Privileges control access to computer and domain resources, and can override permissions that have been set on specific objects.

An example of a logon right is the ability to log on to a computer locally. An example of a privilege is the ability to shut down the computer. Both types of user rights are assigned by administrators to individual users or groups as part of the security settings for the computer. For a summary of the prescribed settings in this chapter, see the Microsoft® Excel® workbook "Windows Default Security and Services Configuration" that is included with this guide. This workbook documents the default user rights assignment settings.

Note: Internet Information Server (IIS) expects certain user rights to be assigned to the built-in accounts that it uses. The user rights assignment settings in this chapter identify which rights IIS requires; for more information about these requirements, see the "IIS and Built-In Accounts (IIS 6.0)" list at www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/3648346f-e4f5-474b-86c7-5a86e85fa1ff.mspx.

User Rights Assignment Settings

You can configure the user rights assignment settings in the following location within the Group Policy Object Editor:

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

Access this computer from the network

This policy setting determines whether users can connect to the computer from the network. This capability is required by a number of network protocols, including Server Message Block (SMB)-based protocols, NetBIOS, Common Internet File System (CIFS), and Component Object Model Plus (COM+).

The possible values for the Access this computer from the network setting are:

- A user-defined list of accounts
- Not Defined
Vulnerability

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 and some shared folders have both share and NTFS file system (NTFS) permissions configured so that the same group has read access, then anyone in the group will be able to view files in those shared folders. However, this situation is unlikely for new installations of Microsoft Windows Server™ 2003 with Service Pack 1 (SP1), because the default share and NTFS permissions in Windows Server 2003 do not include the **Everyone** group. This vulnerability may have a higher level of risk for computers that you upgrade from Windows NT® 4.0 or Windows 2000, because the default permissions for these operating systems are not as restrictive as the default permissions in Windows Server 2003.

Countermeasure

Restrict the **Access this computer from the network** user right to only those users who require access to the server. For example, if you configure this policy setting to the **Administrators** and **Users** groups, users who log on to the domain will be able to access resources shared from servers in the domain if members of the **Domain Users** group are included in the local **Users** group.

Potential 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. 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.

*Act as part of the operating system*

This policy setting determines whether a process can assume the identity of any user and thereby gain access to the resources that the user is authorized to access. Typically, only low-level authentication services require this user right. Note that potential access is not limited to what is associated with the user by default. The calling process might request that arbitrary additional privileges be added to the access token. The calling process might also build an access token that does not provide a primary identity for auditing in the system event logs.

The possible values for the **Act as part of the operating system** setting are:

- A user-defined list of accounts
- Not Defined

Vulnerability

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.
Chapter 4: User Rights

Countermeasure
Restrict the Act as part of the operating system user right to as few accounts as possible—it should not even be assigned to the Administrators group under typical circumstances. When a service requires this user right, configure the service to log on with the Local System account, which has this privilege inherently. Do not create a separate account and assign this user right to it.

Potential 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.

Add workstations to domain
This policy setting determines whether a user can add a computer to a specific domain. For it to take effect, it must be assigned so that it applies to at least one domain controller. A user who is assigned this user right can add up to ten workstations to the domain. Users can also join a computer to a domain if they have the Create Computer Objects permission for an organizational unit (OU) or for the Computers container in the Active Directory® directory service. Users who are assigned this permission can add an unlimited number of computers to the domain regardless of whether they have the Add workstations to domain user right.

The possible values for the Add workstations to domain setting are:
• A user-defined list of accounts
• Not Defined

Vulnerability
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 their computer and then add the computer to the domain. They would know the password for the local administrator account, and they could log on with that account and then add their domain account to the local Administrators group.

Countermeasure
Configure the Add workstations to domain setting so that only authorized members of the information technology (IT) team are allowed to add computers to the domain.

Potential 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.
Adjust memory quotas for a process
This policy setting determines whether users can adjust the maximum amount of memory that is available to a process. Although this capability is useful when you need to tune computers, you should consider its potential for abuse. In the wrong hands, it could be used to launch a denial of service (DoS) attack.

The possible values for the Adjust memory quotas for a process setting are:

- A user-defined list of accounts
- Not Defined

Vulnerability
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.

Countermeasure
Restrict the Adjust memory quotas for a process user right to users who require it to perform their jobs, such as application administrators who maintain database management systems or domain administrators who manage the organization’s directory and its supporting infrastructure.

Potential 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 to a domain account.

Allow log on locally
This policy setting determines whether a user can start an interactive session on the computer. Users who do not have this right are still able to start a remote interactive session on the computer if they have the Allow logon through Terminal Services right.

The possible values for the Allow log on locally setting are:

- A user-defined list of accounts
- Not Defined

Vulnerability
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 execute malicious code to elevate their privileges.
Countermeasure

For domain controllers, only assign the Allow log on locally user right to the Administrators group. For other server roles, you may choose to add Backup Operators and Power Users. For end-user computers you should also assign this right to the Users group.

Alternatively, you can assign groups such as Account Operators, Server Operators, and Guests to the Deny Log on Locally user right.

Potential 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.

Allow log on through Terminal Services

This policy setting determines whether users can log on to the computer through a Remote Desktop connection. You should not assign this user right to additional users or groups. Instead, it is a best practice to add users to or remove users from the Remote Desktop Users group to control who can open a Remote Desktop connection to the computer.

The possible values for the Allow log on through Terminal Services setting are:

- A user-defined list of accounts
- Not Defined

Vulnerability

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 execute malicious code to elevate their privileges.

Countermeasure

For domain controllers, only assign the Allow log on through Terminal Services user right to the Administrators group. For other server roles and end-user computers, add the Remote Desktop Users group. For Terminal Servers that do not run in Application Server mode, ensure that only authorized IT personnel who need to manage the computers remotely belong to either of these groups.

Warning: For Terminal Servers that run in Application Server mode, ensure that only users who require access to the server have accounts that belong to the Remote Desktop Users group, because this built-in group has this logon right by default.

Alternatively, you can assign the Deny Logon Through Terminal Services user right to groups such as Account Operators, Server Operators, and Guests. However, be careful when you use this method because you could block access to legitimate administrators who also happen to belong to a group that has the Deny Logon Through Terminal Services user right.
Potential 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.

**Back up files and directories**

This policy setting determines whether users can circumvent file and directory permissions to back up the computer. This user right is effective only when an application attempts access through the NTFS backup application programming interface (API) through a backup utility such as NTBACKUP.EXE. Otherwise, standard file and directory permissions apply.

The possible values for the Back up files and directories setting are:

- A user-defined list of accounts
- Not Defined

**Vulnerability**

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.

**Countermeasure**

Restrict the Back up files and directories user right to members of the IT team who need to be able to backup organizational data as part of their day-to-day job responsibilities. If you are using backup software that runs under specific service accounts, only these accounts (and not the IT staff) should have the Back up files and directories user right.

Potential 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.

**Bypass traverse checking**

This policy setting determines whether users can pass through folders without being checked for the special access permission “Traverse Folder” when they navigate an object path in the NTFS file system or in the registry. This user right does not allow the user to list the contents of a folder; it only allows the user to traverse folders.

The possible values for the Bypass traverse checking setting are:

- A user-defined list of accounts
- Not Defined
Chapter 4: User Rights

Vulnerability

The default configuration for the **Bypass traverse checking** setting is to allow anyone to bypass traverse checking, and experienced Windows system administrators configure file system access control list (ACLs) accordingly. 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, they 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.

Countermeasure

Organizations that are extremely concerned about security may want to remove the **Everyone** group, or perhaps even the **Users** group, from the list of groups with the **Bypass traverse checking** user right. Taking explicit control over traversal assignments can be a very effective way to control access to sensitive information. (Also, the **Access-based Enumeration** feature that was added in Windows Server 2003 SP1 can be used. If you use access–based enumeration, users cannot see any folder or file to which they do not have access. For more information about this feature, see www.microsoft.com/technet/prodtechnol/windowsserver2003/library/BookofSP1/f04862a9-3e37-4f8c-ba87-917f4fb5b42c.mspx.)

Potential 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, Microsoft recommends 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.) This guide recommends that you leave this policy setting at its default configuration.

*Change the system time*

This policy setting determines whether users can adjust the time on the computer's internal clock. It is not required to change the time zone or other display characteristics of the system time.

The possible values for the **Change the system time** setting are:

- A user-defined list of accounts
- Not Defined

Vulnerability

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.

**Countermeasure**

Restrict the *Change the system time* user right to users with a legitimate need to change the system time, such as members of the IT team.

**Potential 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.

**Create a page file**

This policy setting determines whether users can create and change the size of a page file. Specifically, it determines whether they can specify a page file size for a particular drive in the *Performance Options* box that is located on the *Advanced* tab of the *System Properties* dialog box.

The possible values for the *Create a page file* setting are:

- A user-defined list of accounts
- Not Defined

**Vulnerability**

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.

**Countermeasure**

Restrict the *Create a page file* user right to members of the *Administrators* group.

**Potential Impact**

None. This is the default configuration.
Chapter 4: User Rights

Create a token object

This policy setting determines whether a process can create a token, which it can then use to gain access to any local resources when the process uses NtCreateToken() or other token-creation APIs.

The possible values for the Create a token object setting are:

- A user-defined list of accounts
- Not Defined

Vulnerability

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 reconnects. A user with the ability to create or modify tokens can change the level of access for any currently logged on account. They could escalate their own privileges or create a DoS condition.

Countermeasure

Do not assign the Create a token object user right to any users. Processes that require this user right should use the System account, which already includes it, instead of a separate user account that has this user right assigned.

Potential Impact

None. This is the default configuration.

Create global objects

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.

The possible values for the Create global objects setting are:

- A user-defined list of accounts
- Not Defined

Vulnerability

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.

Countermeasure

Restrict the Create global objects user right to members of the local Administrators and Service groups.

Potential Impact

None. This is the default configuration.
**Create permanent shared objects**

This policy setting determines whether users can create directory objects in the object manager. Users who have this capability can create permanent shared objects, including devices, semaphores, and mutexes. This user right is useful to kernel-mode components that extend the object namespace, and they have this user right inherently. Therefore, it is typically not necessary to specifically assign this user right to any users.

The possible values for the *Create permanent shared objects* setting are:

- A user-defined list of accounts
- Not Defined

**Vulnerability**

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

**Countermeasure**

Do not assign the *Create permanent shared objects* user right to any users. Processes that require this user right should use the System account (which already includes this user right) instead of a separate user account.

**Potential Impact**

None. This is the default configuration.

**Debug programs**

This policy setting determines whether users can open or attach to any process, even those that they do not own. This user right provides access to sensitive and critical operating system components.

The possible values for the *Debug programs* setting are:

- A user-defined list of accounts
- Not Defined

**Vulnerability**

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 effect rootkit code insertions. By default, the *Debug programs* user right is assigned only to administrators, which helps to mitigate the risk from this vulnerability.

**Countermeasure**

Revoke the *Debug programs* user right from all users and groups that do not require it.

**Potential Impact**

If you revoke this user right, no one will be able to debug programs. However, typical circumstances rarely require this capability on production computers. If a problem arises
that requires an application to be debugged on a production server temporarily, you can
move the server to a different OU 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, Windows Clustering will fail. For additional information about how
to configure Windows Clustering in conjunction with computer hardening, see Microsoft
Knowledge Base article 891597, “How to apply more restrictive security settings on a
Windows Server 2003–based cluster server” at

Utilities that are used to manage processes will be unable to affect processes that are not
owned by the person who runs the utilities. For example, the Windows Server 2003
Resource Kit tool Kill.exe requires this user right for an administrator to terminate
processes that they did not launch.

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 Microsoft Knowledge Base article 830846,
“Windows Product Updates may stop responding or may use most or all the CPU

**Deny access to this computer from the network**

This policy setting determines whether users have the ability to connect to the computer
from the network.

The possible values for the **Deny access to this computer from the network** setting
are:

- A user-defined list of accounts
- Not Defined

**Vulnerability**

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. You can
explicitly deny this user right to high-risk accounts (such as the local Guest account and
other accounts that have no business need to access the computer over the network) to
provide an additional layer of protection.

**Countermeasure**

Assign the **Deny access to this computer from the network** user right to the following
accounts:

- ANONYMOUS LOGON
- The built-in local Administrator account
- The local Guest account
- The built-in Support account
- All service accounts
An important exception to this list is any service accounts that are used to launch services that need to connect to the computer over the network. For example, if you have configured a shared folder for Web servers to access and present content within that folder through a Web site, you may need to allow the account that runs IIS to log on to the server with the shared folder through the network. This user right is particularly effective when you need to configure servers and workstations on which sensitive information is handled because of regulatory compliance concerns.

Potential 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.

Deny log on as a batch job

This policy setting determines whether users can log on through a batch-queue facility, which is the feature in Windows Server 2003 that is used to schedule and launch jobs automatically one or more times in the future. This user right is needed for any accounts that are used to launch scheduled jobs by means of the Task Scheduler.

The possible values for the Deny log on as a batch job setting are:

- A user-defined list of accounts
- Not Defined

Vulnerability

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.

Countermeasure

Assign the Deny log on as a batch job user right to the built-in Support account and the local Guest account.

Potential 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.
**Deny log on as a service**

This policy setting determines whether users can log on as a service.

The possible values for the **Deny log on as a service** setting are:

- A user-defined list of accounts
- Not Defined

**Vulnerability**

Accounts that can log on as a service could be used to configure and launch new unauthorized services, such as a keylogger or other malware. The benefit of the specified countermeasure is somewhat mitigated 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.

**Countermeasure**

This guide recommends that you not assign the **Deny log on as a service** user right to any accounts, which is the default configuration. Organizations that are extremely concerned about security may wish to assign this user right to groups and accounts that they are certain will never need to log on as a service.

**Potential 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.

**Deny log on locally**

This policy setting determines whether users can log on directly at the computer's keyboard.

The possible values for the **Deny log on locally** setting are:

- A user-defined list of accounts
- Not Defined

**Vulnerability**

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, then unauthorized users might download and execute malicious code that elevates their privileges.
Countermeasure

Assign the **Deny log on locally** user right to the built-in Support account. If you have installed optional components such as ASP.NET, you may want to assign this user right to additional accounts that are required by those components.

**Note:** The Support_388945a0 account enables Help and Support Service interoperability with signed scripts. This account is primarily used to control access to signed scripts that are accessible from within Help and Support Services. Administrators can use this account to delegate the ability for a typical user who does not have administrative access to run signed scripts from links that are embedded within Help and Support Services. These scripts can be programmed to use the Support_388945a0 account credentials instead of the user's credentials to perform specific administrative operations on the local computer that otherwise would not be supported by the typical user's account.

When the delegated user clicks on a link in Help and Support Services, the script will execute under the security context of the Support_388945a0 account. This account has limited access to the computer and is disabled by default.

**Potential Impact**

If you assign the **Deny log on locally** user right to other 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.

**Deny log on through Terminal Services**

This policy setting determines whether users can log on to the computer through a Remote Desktop connection.

The possible values for the **Deny log on through Terminal Services** setting are:

- A user-defined list of accounts
- Not Defined

**Vulnerability**

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, then unauthorized users might download and execute malicious code that elevates their privileges.

**Countermeasure**

Assign the **Deny log on through Terminal Services** logon right to the built-in local Administrator account and all service accounts. If you have installed optional components such as ASP.NET, you may want to assign this logon right to additional accounts that are required by those components.

**Potential 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.
**Enable computer and user accounts to be trusted for delegation**

This policy setting determines whether users can change the Trusted for Delegation setting on a user or computer object in Active Directory. Users or computers that are assigned this user right must also have write access to the account control flags on the object.

Delegation of authentication is a capability that is used by multi-tier client/server applications. It allows a front-end service to use client credentials to authenticate to a back-end service. For this configuration to be possible, both client and server must run under accounts that are trusted for delegation.

The possible values for the Enable computer and user accounts to be trusted for delegation setting are:

- A user-defined list of accounts
- Not Defined

**Vulnerability**

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.

**Countermeasure**

The Enable computer and user accounts to be trusted for delegation user right should only be assigned if there is a clear need for its functionality. When you assign this right, you should investigate the use of constrained delegation to control what the delegated accounts can do.

**Note**: There is no reason to assign this user right to anyone on member servers and workstations that belong to a domain because it has no meaning in those contexts; it is only relevant on domain controllers and stand-alone computers.

**Potential Impact**

None. This is the default configuration.

**Force shutdown from a remote system**

This policy setting determines whether a user can shut down a computer from a remote location on the network.

The possible values for the Force shutdown from a remote system setting are:

- A user-defined list of accounts
- Not Defined

**Vulnerability**

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

Restrict the Force shutdown from a remote system user right to members of the Administrators group or other specifically assigned roles that require this capability (such as non-administrative operations center staff).

Potential 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.

Generate security audits

This policy setting determines whether a process can generate audit records in the Security log. You can use the information in the Security log to trace unauthorized computer access.

The possible values for the Generate security audits setting are:

- A user-defined list of accounts
- Not Defined

Vulnerability

Accounts that can write to the Security log could be used by an attacker to fill that log with meaningless events. If the computer is configured to overwrite events as needed, the attacker could use this method to remove evidence of their unauthorized activities. If the computer is configured to shut down when it is unable to write to the Security log and it is not configured to automatically back up the log files, this method could be used to create a denial of service.

Countermeasure

Ensure that only the Service and Network Service accounts have the Generate security audits user right assigned to them.

Potential Impact

None. This is the default configuration.

Impersonate a client after authentication

The Impersonate a client after authentication user right 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.

Because of these factors, users do not usually need to have this user right assigned.

The possible values for the **Impersonate a client after authentication** setting are:

- A user-defined list of accounts
- Not Defined

**Vulnerability**

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.

**Countermeasure**

On member servers, ensure that only the **Administrators** and **Service** groups have the **Impersonate a client after authentication** user right assigned to them. Computers that run IIS 6.0 must have this user right assigned to the IIS_WPG group (which grants it to the Network Service account).

**Potential 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>.

**Increase scheduling priority**

This policy setting determines whether users can increase the base priority class of a process. (It is not a privileged operation to increase relative priority within a priority class.)

This user right is not required by administrative tools that are supplied with the operating system but might be required by software development tools.

The possible values for the **Increase scheduling priority** setting are:

- A user-defined list of accounts
- Not Defined

**Vulnerability**

A user who is assigned this user right could increase the scheduling priority of a process to Real-Time, which would leave little processing time for all other processes and could lead to a DoS condition.
Countermeasure

Verify that only Administrators have the *Increase scheduling priority* user right assigned to them.

Potential Impact

None. This is the default configuration.

*Load and unload device drivers*

This policy setting determines whether users can dynamically load and unload device drivers. This user right is not required if a signed driver for the new hardware already exists in the Driver.cab file on the computer.

The possible values for the *Load and unload device drivers* setting are:

- A user-defined list of accounts
- Not Defined

Vulnerability

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.

*Note:* You must have this user right, and also be a member of either *Administrators* or *Power Users*, to install a new driver for a local printer or to manage a local printer and configure defaults for options such as duplex printing. The requirement to have both the user right and membership in *Administrators* or *Power Users* is new to Windows XP and Windows Server 2003.

Countermeasure

Do not assign the *Load and unload device drivers* user right to any user or group other than *Administrators* on member servers. On domain controllers, do not assign this user right to any user or group other than *Domain Admins*.

Potential 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.

*Lock pages in memory*

This policy setting determines whether a process can keep data in physical memory, which prevents the computer from paging the data to virtual memory on disk. If you assign this user right, significant degradation of computer performance can occur.

The possible values for the *Lock pages in memory* setting are:

- A user-defined list of accounts
- Not Defined
Chapter 4: User Rights

Vulnerability

Users with the Lock pages in memory user right could assign physical memory to several processes, which could leave little or no RAM for other processes and result in a DoS condition.

Countermeasure

Do not assign the Lock pages in memory user right to any accounts.

Potential Impact

None. This is the default configuration.

Log on as a batch job

This policy setting determines whether users can log on through a batch-queue facility such as the Task Scheduler service. When an administrator uses the Add Scheduled Task wizard to schedule a task to run under a particular user name and password, that user is automatically assigned the Log on as a batch job user right. When the scheduled time arrives, the Task Scheduler service logs the user on as a batch job instead of as an interactive user, and the task runs in the user’s security context.

The possible values for the Log on as a batch job setting are:
• A user-defined list of accounts
• Not Defined

Vulnerability

The Log on as a batch job user right presents a low-risk vulnerability. For most organizations, the default settings are sufficient.

Countermeasure

You should allow the computer to manage this logon right automatically if you want to allow scheduled tasks to run for specific user accounts. If you do not want to use the Task Scheduler in this manner, configure the Log on as a batch job user right for only the Local Service account and the local support account (Support_388945a0). For IIS servers, you should configure this policy locally instead of through domain–based Group Policies so that you can ensure that the local IUSR_<ComputerName> and IWAM_<ComputerName> accounts have this logon right.

Potential 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.
**Log on as a service**

This policy setting determines whether a security principal can log on as a service. Services can be configured to run under the Local System, Local Service, or Network Service accounts, which have a built-in right to log on as a service. Any service that runs under a separate user account must be assigned this user right.

The possible values for the **Log on as a service** setting are:

- A user-defined list of accounts
- Not Defined

**Vulnerability**

**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.

**Countermeasure**

The default set of security principals that have the **Log on as a service** user right is restricted to Local System, Local Service, and Network Service, all of which are built-in local accounts. You should minimize the number of other accounts that have this user right.

**Potential 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.

**Manage auditing and security log**

This policy setting determines whether users can specify object access audit options for individual resources such as files, Active Directory objects, and registry keys. Object access audits are not performed unless you enable them through **Audit Policy**, which is located under **Security Settings, Local Policies**. A user who is assigned this user right can also view and clear the Security event log from Event Viewer.

The possible values for the **Manage auditing and security log** setting are:

- A user-defined list of accounts
- Not Defined

**Vulnerability**

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.
Countermeasure

Ensure that only the local Administrators group has the Manage auditing and security log user right.

Potential Impact

None. This is the default configuration.

Modify firmware environment values

This policy setting determines whether users can modify system environment variables by either a process through an API or by a user through System Properties.

The possible values for the Modify firmware environment values setting are:

• A user-defined list of accounts
• Not Defined

Vulnerability

Anyone who is assigned the Modify firmware environment values user right could configure the settings of a hardware component to cause it to fail, which could lead to data corruption or a DoS condition.

Countermeasure

Ensure that only the local Administrators group is assigned the Modify firmware environment values user right.

Potential Impact

None. This is the default configuration.

Perform volume maintenance tasks

This policy setting determines whether non-administrative or remote users can perform volume or disk management tasks, such as defragment an existing volume, create or remove volumes, and run the Disk Cleanup tool. Windows Server 2003 checks for this user right in a user’s access token when a process that runs in the user’s security context calls SetFileValidData().

The possible values for the Perform volume maintenance tasks setting are:

• A user-defined list of accounts
• Not Defined

Vulnerability

A user who is assigned the Perform volume maintenance tasks user right could delete a volume, which could result in the loss of data or a DoS condition.

Countermeasure

Ensure that only the local Administrators group is assigned the Perform volume maintenance tasks user right.
Potential Impact
None. This is the default configuration.

**Profile single process**
This policy setting determines whether users can sample the performance of an application process. Typically, you do not need 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 through Windows Management Instrumentation (WMI).

The possible values for the **Profile single process** setting are:
- A user-defined list of accounts
- Not Defined

**Vulnerability**
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.

**Countermeasure**
Ensure that only the local **Administrators** group is assigned the **Profile single process** user right.

**Potential 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.

**Profile system performance**
This policy setting determines whether a user can sample the performance of computer system processes. This privilege is required by the MMC Performance snap-in only if it is configured to collect data through WMI. Typically, you do not need this user right to use the Performance snap-in. However, you do need this user right if System Monitor is configured to collect data through WMI.

The possible values for the **Profile system performance** setting are:
- A user-defined list of accounts
- Not Defined

**Vulnerability**
The **Profile system performance** user right 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 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.

**Countermeasure**

Ensure that only the local Administrators group is assigned the Profile system performance user right.

**Potential Impact**

None. This is the default configuration.

---

**Remove computer from docking station**

This policy setting determines whether the user of a portable computer can click Eject PC on the Start menu to undock the computer.

The possible values for the Remove computer from docking station setting are:

- A user-defined list of accounts
- Not Defined

**Vulnerability**

Anyone who has the Remove computer from docking station user right can remove a portable computer from its docking station. The value of this countermeasure is reduced by the following factors:

- If an attacker can restart the computer, they could remove it from the docking station after the BIOS starts but before the operating system launches.
- 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.

**Countermeasure**

Ensure that only the local Administrators and Power Users groups are assigned the Remove computer from docking station user right.

**Potential Impact**

This configuration is the default setting, so it should have little impact. However, if your organization’s users are not members of the Power Users or Administrators groups, they will be unable to remove their own portable computers from their docking stations without shutting them down first. Therefore, you may want to assign the Remove computer from docking station privilege to the local Users group for portable computers.
Replace a process level token

This policy setting determines whether a parent process can replace the access token that is associated with a child process.

The possible values for the Replace a process level token setting are:

- A user-defined list of accounts
- Not Defined

Vulnerability

A user with the Replace a process level token privilege is able to launch processes as other users. They could use this method to hide their unauthorized actions on the computer. (On Windows 2000 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 chapter.)

Countermeasure

For member servers, ensure that only the Local Service and Network Service accounts have the Replace a process level token user right.

Potential 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.

Restore files and directories

This policy setting determines whether a user can circumvent file and directory permissions when they restore backed up files and directories and whether they can set any valid security principal as the owner of an object.

The possible values for the Restore files and directories setting are:

- A user-defined list of accounts
- Not Defined

Vulnerability

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. An attacker could overwrite executable files that are used by legitimate administrators or system services with versions that include malicious code to grant themselves elevated privileges, compromise data, or install backdoors for continued access to the computer.

Note: Even if this 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.
Countermeasure

Ensure that only the local Administrator group is assigned the Restore files and directories user right, unless your organization has clearly defined roles for backup and for restore personnel.

Potential 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.

**Shut down the system**

This policy setting determines whether a user can shut down the local computer.

The possible values for the Shut down the system setting are:
- A user-defined list of accounts
- Not Defined

Vulnerability

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 the accounts and groups that 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 Single–Master Operations (FSMO) roles you can disable key domain functionality, such as processing logons for new passwords—the Primary Domain Controller (PDC) Emulator role.

Countermeasure

Ensure that only Administrators and Backup Operators are assigned the Shut down the system user right on member servers, and that only Administrators have it on domain controllers.

Potential 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.

**Synchronize directory service data**

This policy setting determines whether a process can read all objects and properties in the directory, regardless of the protection on the objects and properties. This privilege is required to use LDAP directory synchronization (dirsync) services.

The possible values for the Synchronize directory service data setting are:
- A user-defined list of accounts
- Not Defined
Vulnerability
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. An attacker who has 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.

Countermeasure
Ensure that no accounts are assigned the Synchronize directory service data user right.

Potential Impact
None. This is the default configuration.

Take ownership of files or other objects
This policy setting determines whether a user can take ownership of any securable object in the computer, including Active Directory objects, NTFS files and folders, printers, registry keys, services, processes, and threads.

The possible values for the Take ownership of files or other objects setting are:
• A user-defined list of accounts
• Not Defined

Vulnerability
Any user with the Take ownership of files or other objects user right can take control of any object, regardless of the permissions on that object, and then make any changes they wish to that object. Such changes could result in exposure of data, corruption of data, or a DoS condition.

Countermeasure
Ensure that only the local Administrators group has the Take ownership of files or other objects user right.

Potential Impact
None. This is the default configuration.
More Information

The following links provide additional information about user rights assignment in Windows Server 2003 and Windows XP.

- Extensive information about assigning user rights with the SCE is available in the "User Rights Assignment" section of the Security Configuration Editor online help for Windows Server 2003 at www.microsoft.com/technet/prodtechnol/windowsserver2003/library/serverhelp/71b2772f-e3c0-4134-b7f0-54c244ee9aef.mspx.

- Detailed information about local user rights assignments on Windows XP computers is available in the help topic "To assign user rights for your local computer" at www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/lpe_assign_user_right.mspx.

- For more information about user rights assignments in Windows XP, see the "User Rights Assignment" section of the online Windows XP Professional documentation at www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/uratopnode.mspx.

- For more information about how to customize the Security Configuration Editor user interface, see the Microsoft Knowledge Base article "How to Add Custom Registry Settings to Security Configuration Editor" at http://support.microsoft.com/?scid=214752.

- For more information about how to create custom administrative template files in Windows, see the Microsoft Knowledge Base article "How to: Create Custom Administrative Templates in Windows 2000" at http://support.microsoft.com/?scid=323639.
Security Options

The Security Options section of Group Policy enables or disables computer security settings for digital data signatures, Administrator and Guest account names, access to floppy disk and CD-ROM drives, driver installation behavior, and logon prompts. The Microsoft® Excel® workbook "Windows Default Security and Services Configuration" (included with the downloadable version of this guide) documents the default settings.

Security Options Settings

You can configure the security options settings in the following location within the Group Policy Object Editor:

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options
```

**Accounts: Administrator account status**

This policy setting enables or disables the Administrator account for normal operational conditions. If you start a computer in safe mode, the Administrator account is always enabled, regardless of how you configure this policy setting.

The possible values for the **Accounts: Administrator account status** setting are:

- Enabled
- Disabled
- Not Defined

**Vulnerability**

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.
**Countermeasure**

Configure the **Accounts: Administrator account status** setting to **Disabled** so that the built-in Administrator account is no longer usable in a normal system startup.

**Potential 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.

**Accounts: Guest account status**

This policy setting determines whether the Guest account is enabled or disabled.

The possible values for the **Accounts: Guest account status** setting are:

- Enabled
- Disabled
- Not Defined

**Vulnerability**

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.

**Countermeasure**

Configure the **Accounts: Guest account status** setting to **Disabled** so that the built-in Guest account is no longer usable.

**Potential Impact**

All network users will need to authenticate before they can access shared resources. If you disable the Guest account and the **Network Access: Sharing and Security Model** option is set to **Guest Only**, network logons, such as those performed by the Microsoft Network Server (SMB Service), will fail. This policy setting should have little impact on most organizations because it is the default setting in Microsoft Windows® 2000, Windows XP, and Windows Server™ 2003.
Accounts: Limit local account use of blank passwords to console logon only

This policy setting determines whether remote interactive logons by network services such as Terminal Services, Telnet, and File Transfer Protocol (FTP) are allowed for local accounts that have blank passwords. If you enable this policy setting, a local account must have a non-blank password to perform an interactive or network logon from a remote client.

The possible values for the Accounts: Limit local account use of blank passwords to console logon only setting are:

- Enabled
- Disabled
- Not Defined

Note: This policy setting does not affect interactive logons that are performed physically at the console or logons that use domain accounts.

Caution: It is possible for third-party applications that use remote interactive logons to bypass this policy setting.

Vulnerability

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 a user with the ability to create new accounts bypasses 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.

Countermeasure

Enable the Accounts: Limit local account use of blank passwords to console logon only setting.

Potential Impact

None. This is the default configuration.

Accounts: Rename administrator account

This policy setting determines whether a different account name is associated with the SID for the Administrator account.

The possible values for the Accounts: Rename administrator account setting are:

- User-defined text
- Not Defined

Vulnerability

The Administrator account exists on all computers that run the Windows 2000, Windows Server 2003, or Windows XP Professional operating systems. If you rename
this account, it is slightly more difficult for unauthorized persons to guess this privileged user name and password combination.

The built-in Administrator account cannot be locked out, regardless of how many times an attacker might use a bad password. This capability makes the Administrator account a popular target for brute force attacks that attempt to guess passwords. The value of this countermeasure is lessened because this account has a well-known SID, and there are third-party tools that allow authentication by using the SID rather than the account name. Therefore, even if you rename the Administrator account, an attacker could launch a brute force attack by using the SID to log on.

**Countermeasure**

Specify a new name in the **Accounts: Rename administrator account** setting to rename the Administrator account.

**Note:** In later chapters this policy setting is not configured in the security templates, nor is a new username for the account suggested in the guide. The templates omit this policy setting so that the numerous organizations that use this guidance would not implement the same new username in their environments.

**Potential Impact**

You will have to inform users who are authorized to use this account of the new account name. (The guidance for this setting assumes that the Administrator account was not disabled, which was recommended earlier in this chapter.)

**Accounts: Rename guest account**

The **Accounts: Rename guest account** setting determines whether a different account name is associated with the SID for the Guest account.

The possible values for this Group Policy setting are:

- User-defined text
- Not Defined

**Vulnerability**

The Guest account exists on all computers that run the Windows 2000, Windows Server 2003, or Windows XP Professional operating systems. If you rename this account, it is slightly more difficult for unauthorized persons to guess this privileged user name and password combination.

**Countermeasure**

Specify a new name in the **Accounts: Rename guest account** setting to rename the Guest account.

**Note:** In later chapters this policy setting is not configured in the security templates, nor is a new username for the account suggested in the guide. The templates omit this policy setting so that the numerous organizations that use this guidance would not implement the same new username in their environments.

**Potential Impact**

There should be little impact, because the Guest account is disabled by default in Windows 2000, Windows XP, and Windows Server 2003.
Audit: Audit the access of global system objects

If you enable this policy setting, a default system access control list (SACL) will be applied when the computer creates system objects such as mutexes, events, semaphores, and MS-DOS® devices. If you also enable the Audit object access audit setting as described in Chapter 3 of this guide, access to these system objects is audited.

Global system objects, also known as “base system objects” or “base named objects,” are ephemeral kernel objects that have had names assigned to them by the application or system component that created them. These objects are most commonly used to synchronize multiple applications or multiple parts of a complex application. Because they have names, these objects are global in scope, and therefore visible to all processes on the computer. These objects all have a security descriptor but typically have a NULL SACL. If you enable this policy setting at startup time, the kernel will assign a SACL to these objects when they are created.

The possible values for the Audit: Audit the access of global system objects setting are:

- Enabled
- Disabled
- Not Defined

Vulnerability

A globally visible named object, if incorrectly secured, could be acted upon by a malicious program that knew 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 a malicious program 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.

Countermeasure

Enable the Audit: Audit the access of global system objects setting.

Potential 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 event log to record numerous events of little significance. This policy setting can only be enabled or disabled, and there is no way to filter which events are recorded and which are not. 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 from a configuration of Enabled for this policy setting.

Audit: Audit the use of Backup and Restore privilege

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 policy settings, an audit event is generated for every file that is backed up or restored.
If you enable this policy setting in conjunction with the **Audit privilege use** setting, any exercise of user rights in the Security log is recorded. If you disable this policy setting, actions by users of Backup or Restore privileges are not audited, even if **Audit privilege use** is enabled.

The possible values for the **Audit: Audit the use of Backup and Restore privilege** setting are:

- Enabled
- Disabled
- Not Defined

**Vulnerability**

If you enable this option when the **Audit privilege use** setting is also enabled, an audit event is generated for every file that is backed up or restored. This information could help you to identify an account that was used to accidentally or maliciously restore data in an unauthorized manner.

**Countermeasure**

Enable the **Audit use of Backup and Restore privilege** setting. Alternatively, implement automatic log backup by configuring the AutoBackupLogFiles registry key, which is 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.

**Potential 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.

**Audit: Shut down system immediately if unable to log security audits**

This policy setting determines whether the computer shuts down if it is unable to log security events. The Trusted Computer System Evaluation Criteria (TCSEC)-C2 and Common Criteria certifications require that the computer be able to prevent the occurrence of auditable events if the audit system is unable to log them. The way that Microsoft chose to meet this requirement is to halt the computer and display a stop message in the case of a failure of the audit system. If you enable this policy setting, the computer stops if a security audit cannot be logged for any reason. Typically, an event fails to be logged when the Security event log is full and its specified retention method is either **Do Not Overwrite Events** or **Overwrite Events by Days**.
When this policy setting is enabled, the following Stop message displays if the security log is full and an existing entry cannot be overwritten:

STOP: C0000244 {Audit Failed}

An attempt to generate a security audit failed.

To recover, an administrator must log on, archive the log (optional), clear the log, and disable this option to allow the computer to be restarted. At that point, it may be necessary to manually clear the Security event log before you can configure this policy setting to Enabled.

The possible values for the Audit: Shut down system immediately if unable to log security audits setting are:

- Enabled
- Disabled
- Not Defined

Vulnerability

If the computer is unable to record events to the Security log, then 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 event log messages to purposely force a computer shutdown.

Countermeasure

Enable the Shut down system immediately if unable to log security audits setting.

Potential 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 (NTFS) guarantees its integrity if 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.

**DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL)**

This policy setting allows administrators to define additional computer-wide access controls that govern access to all Distributed Component Object Model (DCOM)–based applications on a computer. These controls restrict call, activation, or launch requests on the computer. The simplest way to think about these access controls is as an additional access check call that is done against a computer-wide access control list (ACL) on each call, activation, or launch of any COM server on the computer. If the access check fails, the call, activation, or launch request will be denied. (This check is in addition to any
Threats and Countermeasures

access check that is run against the server-specific ACLs.) In effect, it provides a minimum authorization standard that must be passed to access any COM server on the computer. The **DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL)** setting controls access permissions to cover call rights.

These computer-wide ACLs provide a way to override weak security settings that are specified by a specific application through CoInitializeSecurity or application-specific security settings. They provide a minimum security standard that must be passed, regardless of the settings of the specific server.

These ACLs provide a centralized location for an administrator to set general authorization policy that applies to all COM servers on the computer.

The **DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL)** setting allows you to specify an ACL in two different ways. You can type in the security descriptor in SDDL, or you can choose users and groups and grant or deny them Local Access and Remote Access permissions. Microsoft recommends that you use the built-in user interface to specify the ACL contents that you want to apply with this setting.

**Vulnerability**

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 modification of 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 access (as explained in the previous section), 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.

**Countermeasure**

To protect individual COM-based applications or services, set the **DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL)** setting to an appropriate computer-wide ACL.

**Potential Impact**

Windows XP with SP2 and Windows Server 2003 with SP1 implement default COM ACLs as specified in their respective documentation. 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 will 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.

**Note:** For more information about the default COM machine access restrictions that are applied in Windows XP with SP2, see the "Managing Windows XP Service Pack 2 Features Using Group Policy" guide at www.microsoft.com/technet/prodtechnol/winxppro/maintain/mangxpss2/mngsepcs.mspx.

For information about the restrictions that are applied in Windows Server 2003 with SP1, see the "DCOM Security Enhancements" section in the "Changes to Functionality in Microsoft Windows Server 2003 Service Pack 1" guide at www.microsoft.com/technet/prodtechnol/windowsserver2003/library/BookofSP1/ed9975ba-3933-4e28-bcb4-72b80d7865b7.mspx.
For more information about launch permissions, see the "LaunchPermission" page on Microsoft MSDN® at http://go.microsoft.com/fwlink/?LinkId=209244.

**DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL)**

This policy setting is similar to the DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) setting in that it allows administrators to define additional computer-wide access controls that govern access to all DCOM–based applications on a computer. However, the ACLs that are specified in this policy setting control local and remote COM launch requests (not access requests) on the computer. The simplest way to think about this access control is as an additional access check call that is done against a computer-wide ACL on each launch of any COM server on the computer. If the access check fails, the call, activation, or launch request will be denied. (This check is in addition to any access check that is run against the server-specific ACLs.) In effect, it provides a minimum authorization standard that must be passed to launch any COM server on the computer. The earlier policy differs in that it provides a minimum access check that is applied to attempts to access an already launched COM server.

These computer-wide ACLs provide a way to override weak security settings that are specified by a specific application through CoInitializeSecurity or application-specific security settings. They provide a minimum security standard that must be passed, regardless of the settings of the specific COM server. These ACLs provide a centralized location for an administrator to set general authorization policy that applies to all COM servers on the computer.

The DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) setting allows you to specify an ACL in two different ways. You can type in the security descriptor in SDDL, or you can choose users and groups and grant or deny them Local Access and Remote Access permissions. Microsoft recommends that you use the built-in user interface to specify the ACL contents that you want to apply with this setting.

**Vulnerability**

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 modification of 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 (as explained in the previous section), 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.

**Countermeasure**

To protect individual COM-based applications or services, set the DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) setting to an appropriate machine-wide ACL.
Potential Impact

Windows XP with SP2 and Windows Server 2003 with SP1 implement default COM ACLs as specified in their respective documentation. 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 will 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.

Note: For more information about the default COM machine launch restrictions that are applied in Windows XP with SP2, see the "Managing Windows XP Service Pack 2 Features Using Group Policy" guide at www.microsoft.com/technet/prodtechnol/winxppro/maintain/mangxpssp2/mngsecp.mspx.

For information about the restrictions that are applied in Windows Server 2003 with SP1, see the "DCOM Security Enhancements" section in the "Changes to Functionality in Microsoft Windows Server 2003 Service Pack 1" guide at www.microsoft.com/technet/prodtechnol/windowsserver2003/library/BookofSP1/ed9975ba-3933-4e28-bcb4-72b80d7865b7.mspx.

For more information about launch permissions, see the "LaunchPermission" page on MSDN at http://go.microsoft.com/fwlink/?LinkId=20924.

Devices: Allow undock without having to log on

This policy setting determines whether a user must log on to request permission to remove a portable computer from a docking station. If you enable this policy setting, users will be able to press a docked portable computer's physical eject button to safely undock the computer. If you disable this policy setting, the user must log on to receive permission to undock the computer. Only users who have the Remove Computer from Docking Station privilege can obtain this permission.

Note: You should only disable this policy setting for portable computers that cannot be mechanically undocked. Computers that can be mechanically undocked can be physically removed by the user whether or not they use the Windows undocking functionality.

The possible values for the Devices: Allow undock without having to log on setting are:

- Enabled
- Disabled
- Not Defined

Vulnerability

If this policy setting is enabled, anyone with physical access to portable computers in their docking station could remove them and possibly tamper with them. For computers that do not have docking stations, this policy setting will have no impact.

Countermeasure

Disable the Devices: Allow undock without having to log on setting.

Potential Impact

Users who have docked their computers will have to log on to the local console before they can undock their computers.
**Devices: Allowed to format and eject removable media**

This policy setting determines who is allowed to format and eject removable media.

The possible values for the **Devices: Allowed to format and eject removable media** setting are:

- Administrators
- Administrators and Power Users
- Administrators and Interactive Users
- Not Defined

**Vulnerability**

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.

**Countermeasure**

Configure the **Allowed to format and eject removable media** setting to Administrators.

**Potential Impact**

Only Administrators will be able to eject NTFS-formatted removable media.

**Devices: Prevent users from installing printer drivers**

For a computer to print to a network printer, that network printer driver must be installed on the local computer. The **Devices: Prevent users from installing printer drivers** setting determines who can install a printer driver as part of adding a network printer. If you enable this policy setting, only members of the Administrators and Power Users groups are allowed to install a printer driver when they add a network printer. If you disable this policy setting, any user can install printer drivers when they add a network printer. This policy setting prevents typical users from downloading and installing untrusted printer drivers.

**Note:** This policy setting has no impact if an administrator has configured a trusted path to download drivers. If you use trusted paths, the print subsystem attempts to use the trusted path to download the driver. If the trusted path download succeeds, the driver is installed on behalf of any user. If the trusted path download fails, the driver is not installed and the network printer is not added.

The possible values for the **Devices: Prevent users from installing printer drivers** setting are:

- Enabled
- Disabled
- Not Defined
Vulnerability

It may be appropriate in some organizations to allow users to install printer drivers on their own workstations. However, you should not allow users to do so on servers. Printer driver installation on a server may unintentionally cause the computer to become less stable. Only Administrators should have this privilege on servers. A malicious user could install inappropriate printer drivers in a deliberate attempt to damage the computer, or a user might accidentally install malicious code that masquerades as a printer driver.

Countermeasure

Configure the Devices: Prevent users from installing printer drivers setting to Enabled.

Potential 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.

Devices: Restrict CD-ROM access to locally logged-on user only

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. If this policy setting is enabled and no one is logged on interactively, the CD-ROM can be accessed over the network.

The possible values for the Devices: Restrict CD-ROM access to locally logged-on user only setting are:

- Enabled
- Disabled
- Not Defined

Vulnerability

A remote user could potentially access a mounted CD-ROM that contain sensitive information. This risk is small, because CD-ROM drives are not automatically made available as network shares; 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.

Countermeasure

Enable the Restrict CD-ROM drive access to locally logged-on user only setting.

Potential Impact

Users who connect to the server over the network will not be able to use any CD-ROM 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-ROM drive will fail. For example, the Volume Shadow Copy service attempts to access all CD-ROM and floppy 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 utility
to fail if volume shadow copies were specified for the backup job. Any third-party 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.

**Devices: Restrict floppy access to locally logged-on user only**

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 can be accessed over the network.

The possible values for the Devices: Restrict floppy access to locally logged-on user only setting are:

- Enabled
- Disabled
- Not Defined

**Vulnerability**

A remote user could potentially access a mounted floppy that contains sensitive information. This risk is small because floppy drives are not automatically made available as network shares; 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.

**Countermeasure**

Enable the Restrict floppy access to locally logged-on user only setting.

**Potential 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 drives will fail. For example, the Volume Shadow Copy service attempts to access all CD-ROM and floppy 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 utility to fail if volume shadow copies were specified for the backup job. Any third-party backup products that use volume shadow copies will also fail.
Devices: Unsigned driver installation behavior

This policy setting determines what happens when an attempt is made to install a device driver that has not been certified and signed by the Windows Hardware Quality Lab (WHQL) by means of the Setup application programming interface (API).

The possible values for the Devices: Unsigned driver installation behavior setting are:
- Silently succeed
- Warn but allow installation
- Do not allow installation
- Not Defined

Vulnerability

This policy setting prevents the installation of unsigned drivers, or warns the administrator that unsigned driver software is about to be installed. This capability can prevent use of the Setup API to install drivers that have not been certified to run on Windows XP or Windows Server 2003. 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.

Countermeasure

Configure the Devices: Unsigned driver installation behavior setting to Warn but allow installation, which is the default configuration for Windows XP with SP2. The default configuration for Windows Server 2003 is Not Defined.

Potential 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.

Domain controller: Allow server operators to schedule tasks

This policy setting determines whether server operators are allowed to submit jobs by means of the AT schedule facility.

Note: This security option setting only affects the AT schedule facility. It does not affect the Task Scheduler facility.

The possible values for the Domain controller: Allow server operators to schedule tasks setting are:
- Enabled
- Disabled
- Not Defined
Vulnerability

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.

Countermeasure

Disable the Domain controller: Allow server operators to schedule tasks setting.

Potential 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 they set up the job.

Domain controller: LDAP server signing requirements

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

The possible values for the Domain controller: LDAP server signing requirements setting are:

- **None.** Data signatures are not required to bind with the server. If the client requests data signing, the server supports it.
- **Require signature.** The LDAP data-signing option must be negotiated unless Transport Layer Security/Secure Socket Layer (TLS/SSL) is in use.
- **Not Defined.**

Vulnerability

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.

Countermeasure

Configure the Domain controller: LDAP server signing requirements setting to Require signature.

Potential Impact

Clients that do not support LDAP signing will be unable to execute LDAP queries against the domain controllers. All Windows 2000–based computers in your organization that are
managed from Windows Server 2003 or Windows XP–based computers and that use Windows NT® Challenge/Response (NTLM) authentication must have Windows 2000 Service Pack 3 (SP3) installed. Alternatively, these clients must have the registry change that is described in the Microsoft Knowledge Base article Q325465 "Windows 2000 domain controllers require SP3 or later when using Windows Server 2003 administration tools," which is available at http://support.microsoft.com/default.aspx?scid=325465. Also, some third-party 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.

**Domain controller: Refuse machine account password changes**

This policy setting determines whether or not a domain controller will accept password change requests for computer accounts.

The possible values for the **Domain controller: Refuse machine account password changes** setting are:

- Enabled
- Disabled
- Not Defined

**Vulnerability**

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.

**Countermeasure**

Disable the **Domain controller: Refuse machine account password changes** setting.

**Potential Impact**

None. This is the default configuration.

**Domain member: Digitally encrypt or sign secure channel data (multiple related settings)**

The following policy settings determine whether a secure channel can be established with a domain controller that cannot sign or encrypt secure channel traffic:

- Domain member: Digitally encrypt or sign secure channel data (always)
- Domain member: Digitally encrypt secure channel data (when possible)
- Domain member: Digitally sign secure channel data (when possible)

If you enable the **Domain member: Digitally encrypt or sign secure channel data (always)** setting, a secure channel cannot be established with any domain controller that cannot sign or encrypt all secure channel data.

To protect authentication traffic from man-in-the-middle, replay, and other types of network attacks, Windows–based computers create a communication channel through
NetLogon called Secure Channels. These channels authenticate computer accounts, and they also authenticate user accounts when a remote user connects to a network resource and the user account exists in a trusted domain. This authentication is called pass-through authentication, and it allows a computer that has joined a domain to have access to the user account database in its domain and in any trusted domains.

**Note:** To enable the **Domain member: Digitally encrypt or sign secure channel data (always)** setting on a member workstation or server, all domain controllers in the domain that the member belongs to must be able to sign or encrypt all secure channel data. This requirement means that all such domain controllers must run Windows NT 4.0 with Service Pack 6a or a later version of the Windows operating system.

If you enable the **Domain member: Digitally encrypt or sign secure channel data (always)** setting, the **Domain member: Digitally sign secure channel data (when possible)** setting is automatically enabled.

The possible values for this policy setting are:

- Enabled
- Disabled
- Not Defined

**Vulnerability**

When a Windows Server 2003, Windows XP, Windows 2000, or Windows NT 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.

**Countermeasure**

- Configure the **Domain member: Digitally encrypt or sign secure channel data (always)** setting to **Enabled**.
- Configure the **Domain member: Digitally encrypt secure channel data (when possible)** setting to **Enabled**.
- Configure the **Domain member: Digitally sign secure channel data (when possible)** setting to **Enabled**.

**Potential 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:
Threats and Countermeasures

• The ability to create or delete down-level trust relationships will be disabled.
• Logons from down-level clients will be disabled.
• The ability to authenticate other domains’ users from a down-level 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 down-level clients and applications will not be affected.

Domain member: Disable machine account password changes

This policy setting determines whether a domain member periodically changes its computer account password. If you enable this policy setting, the domain member cannot change its computer account password. If you disable this policy setting, the domain member is allowed to change its computer account password as specified by the Domain Member: Maximum age for computer account password setting, which is every 30 days by default.

Caution: Do not enable this policy setting. Computer account passwords are used to establish secure channel communications between members and domain controllers and, within the domain, between the domain controllers themselves. After such communications are established, the secure channel transmits sensitive information that is needed to make authentication and authorization decisions.

Do not use this policy setting in an attempt to support dual-boot scenarios that use the same computer account. If you want to support such a scenario for two installations that are joined to the same domain, use different computer names for the two installations. This policy setting was added to Windows to make it easier for organizations that stockpile pre-built computers that are put into production months later. It eliminates the need for those computers to rejoin the domain. This policy setting is also sometimes used with imaged computers or those with hardware or software level change prevention. Correct imaging procedures make use of this policy unnecessary for imaged computers.

The possible values for the Domain member: Disable machine account password changes setting are:

• Enabled
• Disabled
• Not Defined

Vulnerability

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

Verify that the **Domain member: Disable machine account password changes** setting is configured to **Disabled**.

Potential Impact

None. This is the default configuration.

**Domain member: Maximum machine account password age**

This policy setting determines the maximum allowable age for a computer account password. This setting also applies to Windows 2000 computers, but it is not available through the Security Configuration Manager tools on these computers.

The possible values for the **Domain member: Maximum machine account password age** setting are:

- A user-defined number of days between 0 and 999
- Not Defined

Vulnerability

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

Countermeasure

Configure the **Domain member: Maximum machine account password age** setting to 30 days.

Potential Impact

None. This is the default configuration.

**Domain member: Require strong (Windows 2000 or later) session key**

This policy setting determines whether a secure channel can be established with a domain controller that cannot encrypt secure channel traffic with a strong, 128-bit, session key. If you enable this policy setting, a secure channel cannot be established with any domain controller that cannot encrypt secure channel data with a strong key. If you disable this policy setting, 64-bit session keys are allowed.

**Note:** To enable this policy setting on a member workstation or server, all domain controllers in the domain to which the member belongs must be able to encrypt secure channel data with a strong, 128-bit, key. In other words, all such domain controllers must run Windows 2000 or a later version of the Windows operating system.
The possible values for the **Domain member: Require strong (Windows 2000 or later) session key** setting are:

- Enabled
- Disabled
- Not Defined

**Vulnerability**

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.)

**Countermeasure**

Configure the **Domain member: Require strong (Windows 2000 or later) session key** setting to **Enabled**.

If you enable this policy setting, all outgoing secure channel traffic will require a strong, Windows 2000 or later encryption key. If you disable this policy setting, the key strength is negotiated. You should only enable this policy setting if the domain controllers in all trusted domains support strong keys. By default, this policy setting is disabled.

**Potential 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.

**Interactive logon: Do not display last user name**

This policy setting determines whether the **Log on to Windows** dialog box displays the name of the last user to log on to the computer. If you enable this policy setting, the name of the last user to successfully log on does not display. If you disable this policy setting, the name of the last user to log on will display.

The possible values for the **Interactive logon: Do not display last user name** setting are:

- Enabled
- Disabled
- Not Defined
Vulnerability

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.

Countermeasure

Configure the Do not display last user name in logon screen setting to Enabled.

Potential Impact

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

Interactive logon: Do not require CTRL+ALT+DEL

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.

The possible values for the Interactive logon: Do not require CTRL+ALT+DEL setting are:

• Enabled
• Disabled
• Not Defined

Vulnerability

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.

Countermeasure

Configure the Disable CTRL+ALT+DEL requirement for logon setting to Disabled.

Potential 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.
Interactive logon: Message text for users attempting to log on

The Interactive logon: Message text for users attempting to log on and the Interactive logon: Message title for users attempting to log on settings are closely related. The first policy setting specifies a text message that displays to users when they log on, and the second policy setting specifies a title that displays in the title bar of the window that contains the text message. Many organizations use this text for legal purposes; for example, to warn users about the ramifications of misuse of company information, or to warn them that their actions may be audited.

Caution: Windows XP Professional adds support for logon banners that can exceed 512 characters in length and that can also contain carriage-return line-feed sequences. However, Windows 2000 clients cannot interpret and display these messages. You must use a Windows 2000 computer to create a logon message policy that applies to Windows 2000 computers. If you inadvertently create a logon message policy on a Windows XP Professional computer and you discover that it does not display properly on Windows 2000 computers, do the following:

• Reconfigure the setting to Not Defined.
• Reconfigure the setting using a Windows 2000 computer.

You cannot simply change a Windows XP Professional-defined logon message setting on a Windows 2000 computer. You must first reconfigure the setting to Not Defined.

The possible values for these policy settings are:

• User-defined text
• Not Defined

Vulnerability

Displaying a warning message before logon may help prevent an attack by warning the attacker 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.

Countermeasure

Configure the Message text for users attempting to log on and Message title for users attempting to log on settings to an appropriate value for your organization.

Note: Any warning message that displays should be approved by your organization’s legal and human resources representatives.

Potential Impact

Users will see a message in a dialog box before they can log on to the server console.

Interactive logon: Number of previous logons to cache (in case domain controller is not available)

This policy setting determines the number of different unique users who can log on to a Windows domain by using cached account information. Logon information for domain accounts can be cached locally so that if a domain controller cannot be contacted on subsequent logons, a user can still log on. This policy setting determines the number of unique users whose logon information is cached locally.
If a domain controller is unavailable and a user’s logon information is cached, the user is prompted with the following message:

A domain controller for your domain could not be contacted. You have been logged on using cached account information. Changes to your profile since you last logged on may not be available.

If a domain controller is unavailable and a user’s logon information is not cached, the user is prompted with this message:

The system cannot log you on now because the domain <DOMAIN_NAME> is not available.

The possible values for the Interactive logon: Number of previous logons to cache (in case domain controller is not available) setting are:

- A user-defined number between 0 and 50
- Not Defined

Vulnerability

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.

Countermeasure

Configure the Interactive logon: Number of previous logons to cache (in case domain controller is not available) setting to 0, which disables the local caching of logon information. Additional countermeasures include enforcement of strong password policies and physically secure locations for the computers.

Potential 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.

**Interactive logon: Prompt user to change password before expiration**

This policy setting determines how many days in advance users are warned that their password is about to expire. With this advance warning, the user has time to construct a password that is sufficiently strong.
The possible values for the **Interactive logon: Prompt user to change password before expiration** setting are:

- User defined number of days between 1 and 999
- Not Defined

**Vulnerability**

Microsoft recommends 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.

**Countermeasure**

Configure the **Interactive logon: Prompt user to change password before expiration** setting to 14 days.

**Potential 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.

**Interactive logon: Require Domain Controller authentication to unlock workstation**

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.

The possible values for the **Interactive logon: Require Domain Controller authentication to unlock workstation** setting are:

- Enabled
- Disabled
- Not Defined

**Vulnerability**

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.

**Countermeasure**

Configure the **Interactive logon: Require Domain Controller authentication to unlock workstation** setting to **Enabled** and configure the **Interactive logon: Number of previous logons to cache (in case domain controller is not available)** setting to **0**.

**Potential 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.

**Interactive logon: Require smart card**

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.

The possible values for the **Interactive logon: Require smart card** setting are:

- Enabled
- Disabled
- Not Defined

**Vulnerability**

Requirements to use long, complex passwords for authentication enhance network security, especially if the users must change their passwords regularly. This approach reduces the chance that an attacker will be able to guess a user’s password by means of a brute force attack. However, it is 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. The use of smart cards instead of passwords for authentication dramatically increases security, because current technology makes it almost impossible for an attacker to impersonate another user. Smart cards that require personal identification numbers (PINs) provide two-factor authentication. In other words, the user must both possess the smart card and know its PIN. An attacker who captures the authentication traffic between the user’s computer and the domain controller will find it extremely difficult to decrypt the traffic and, even if they do, the next time the user logs onto the network a new session key will be generated to encrypt traffic between the user and the domain controller.

**Countermeasure**

For sensitive accounts, issue smart cards to users and configure the **Interactive logon: Require smart card** setting to **Enabled**.
Potential Impact

All users will have to use smart cards to log onto the network, which means that the organization will need a reliable public key infrastructure (PKI) as well as smart cards and smart card readers for all users. These requirements are significant challenges, because expertise and resources are required to plan for and deploy these technologies. However, Windows Server 2003 includes Certificate Services, a highly advanced service for implementing and managing certificates. When Certificate Services is combined with Windows XP, features such as automatic user and computer enrollment and renewal become available.

Interactive logon: Smart card removal behavior

This policy setting determines what happens when the smart card for a logged-on user is removed from the smart card reader.

The possible values for the Interactive logon: Smart card removal behavior setting are:

- No Action
- Lock Workstation
- Force Logoff
- Not Defined

Vulnerability

If smart cards are used for authentication, then the computer should automatically lock itself when the card is removed. This approach will prevent malicious users from accessing the computers of users who forget to manually lock their workstations when they are away from them.

Countermeasure

Configure the Smart card removal behavior setting to Lock Workstation.

If you select Lock Workstation in the Properties dialog box for this policy setting, the workstation locks when the smart card is removed. Users can leave the area, take their smart card with them, and still maintain a protected session.

If you select Force Logoff in the Properties dialog box for this policy setting, the user is automatically logged off when the smart card is removed.

Potential Impact

Users will have to re-insert their smart cards and re-enter their PINs when they return to their workstations.
**Microsoft network client and server: Digitally sign communications (four related settings)**

There are four separate settings that relate to digital signatures for Server Message Block (SMB) communications:

- **Microsoft Network Client: Digitally Sign Communications (Always)**
- **Microsoft Network Server: Digitally Sign Communications (Always)**
- **Microsoft Network Client: Digitally Sign Communications (If Server Agrees)**
- **Microsoft Network Server: Digitally Sign Communications (If Client Agrees)**

The possible values for each of these policy settings are:

- Enabled
- Disabled
- Not Defined

**Vulnerability**

Implementation of digital signatures in high security networks helps to prevent the impersonation of clients and servers. This type of impersonation is known as session hijacking, and 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 Microsoft operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place.

**Note:** An alternative countermeasure that could protect all network traffic would be to implement digital signatures with IPsec. There are hardware-based accelerators for IPsec encryption and signing that could be used to minimize the performance impact on the servers’ CPUs. No such accelerators are available for SMB signing.

**Countermeasure**

Configure the settings as follows:

- **Microsoft Network Client: Digitally Sign Communications (Always)** to Disabled
- **Microsoft Network Server: Digitally Sign Communications (Always)** to Disabled
- **Microsoft Network Client: Digitally Sign Communications (If Server Agrees)** to Enabled
- **Microsoft Network Server: Digitally Sign Communications (If Client Agrees)** to Enabled.

Some resources recommend that you configure all of these settings to **Enabled**. However, that configuration may cause slower performance on client computers and prevent communications with legacy SMB applications and operating systems.
Potential Impact

The Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, and Windows XP Professional implementations of the SMB file and print sharing protocol support mutual authentication, which prevents session hijacking attacks and supports message authentication to prevent man-in-the-middle attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server. Implementation of SMB signing may negatively affect performance, because each packet needs to be signed and verified. If you configure computers to ignore all unsigned SMB communications, older applications and operating systems will not be able to connect. If you completely disable all SMB signing, computers will be vulnerable to session hijacking attacks.

**Microsoft network client: Send unencrypted password to third-party SMB servers**

This policy setting allows the SMB redirector to send plaintext passwords to non-Microsoft SMB servers that do not support password encryption during authentication.

The possible values for the **Microsoft network client: Send unencrypted password to third-party SMB servers** setting are:

- Enabled
- Disabled
- Not Defined

Vulnerability

If you enable this policy setting, the server 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 Windows Server 2003.

Countermeasure

Configure the **Microsoft network client: Send unencrypted password to connect to third-party SMB servers** setting to Disabled.

Potential 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.

**Microsoft network server: Amount of idle time required before suspending session**

This policy setting determines the amount of continuous idle time that must pass in a 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. The session automatically re-establishes when client activity resumes. 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.
The possible values for the Microsoft network server: Amount of idle time required before suspending session setting are:

- User-defined period of time in minutes
- Not Defined

**Vulnerability**

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.

**Countermeasure**

Configure the Microsoft network server: Amount of idle time required before disconnecting session setting to 15 minutes.

**Potential Impact**

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

**Microsoft network server: Disconnect clients when logon hours expire**

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.

The possible values for the Microsoft network server: Disconnect clients when logon hours expire setting are:

- Enabled
- Disabled
- Not Defined

**Vulnerability**

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.

**Countermeasure**

Enable the Microsoft network server: Disconnect clients when logon hours expire setting.
Potential 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.

Network access: Allow anonymous SID/Name translation

This policy setting determines whether an anonymous user can request SID attributes for another user.

The possible values for the Network access: Allow anonymous SID/Name translation setting are:

• Enabled
• Disabled
• Not Defined

Vulnerability

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.

Countermeasure

Configure the Network access: Allow anonymous SID/Name translation setting to Disabled.

Potential Impact

Disabled is the default configuration for this policy setting on member computers; therefore it will have no impact on them. The default configuration for domain controllers is Enabled. If you disable this policy setting on domain controllers, legacy computers may be unable to communicate with Windows Server 2003–based domains. For example, the following computers may not work:

• Windows NT 4.0–based Remote Access Service servers.
• Microsoft SQL Servers™ that run on Windows NT 3.x–based or Windows NT 4.0–based computers.
• Remote Access Service or Microsoft SQL servers that run on Windows 2000–based computers and are located in Windows NT 3.x domains or Windows NT 4.0 domains.

Network access: Do not allow anonymous enumeration of SAM accounts

This policy setting determines what additional permissions will be granted for anonymous connections to the computer. Windows allows anonymous users to perform certain activities, such as enumerate the names of domain accounts and network shares. This capability is convenient, for example, when an administrator wants to grant access to users in a trusted domain that does not maintain a reciprocal trust. However, even if this
setting enabled, anonymous users will still have access to any resources that have permissions that explicitly include the special built-in group ANONYMOUS LOGON.

In Windows 2000, a similar policy setting called **Additional Restrictions for Anonymous Connections** managed a registry value called **RestrictAnonymous**, which was located in the \HKLM\SYSTEM\CurrentControlSet\Control\LSA registry key. In Windows Server 2003, the policy settings **Network access: Do not allow anonymous enumeration of SAM accounts** and **Network access: Do not allow anonymous enumeration of SAM accounts and shares** replace the Windows 2000 policy setting. They manage the registry values **RestrictAnonymousSAM** and **RestrictAnonymous**, respectively, which are both located in the \HKLM\System\CurrentControlSet\Control\Lsa registry key.

The possible values for the **Network access: Do not allow anonymous enumeration of SAM accounts** setting are:

- Enabled
- Disabled
- Not Defined

**Vulnerability**

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.)

**Countermeasure**

Configure the **Network access: Do not allow anonymous enumeration of SAM accounts** setting to **Enabled**.

**Potential 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.

**Network access: Do not allow anonymous enumeration of SAM accounts and shares**

This policy setting determines whether anonymous enumeration of Security Accounts Manager (SAM) accounts and shares is allowed. As stated in the previous section, Windows allows anonymous users to perform certain activities, such as enumerate the names of domain accounts and network shares. This capability is convenient, for example, when an administrator wants to grant access to users in a trusted domain that does not maintain a reciprocal trust. You can enable this policy setting if you do not want to allow anonymous enumeration of SAM accounts and shares. However, even if it is enabled, anonymous users will still have access to any resources that have permissions that explicitly include the special built-in group ANONYMOUS LOGON.

In Windows 2000, a similar policy setting called **Additional Restrictions for Anonymous Connections** managed a registry value called **RestrictAnonymous**, which was located in the \HKLM\SYSTEM\CurrentControlSet\Control\LSA registry key. In Windows Server 2003, the policy settings **Network access: Do not allow anonymous**
enumeration of SAM accounts and Network access: Do not allow anonymous enumeration of SAM accounts and shares replace the Windows 2000 policy setting. They manage registry values RestrictAnonymousSAM and RestrictAnonymous, respectively, which are both located in the HKLM\System\CurrentControlSet\Control\Lsa registry key.

The possible values for the Network access: Do not allow anonymous enumeration of SAM accounts and shares setting are:

• Enabled
• Disabled
• Not Defined

Vulnerability
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.

Countermeasure
Configure the Network access: Do not allow anonymous enumeration of SAM accounts and shares setting to Enabled.

Potential 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.

Network access: Do not allow storage of credentials or .NET Passports for network authentication
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.

The possible values for the Network access: Do not allow storage of credentials or .NET Passports for network authentication setting are:

• Enabled
• Disabled
• Not Defined
Vulnerability

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.

Note: The chances of success for this exploit and others that involve hostile code will be reduced significantly for organizations that effectively implement and manage an enterprise antivirus solution combined with sensible software restriction policies. For more information about software restriction policies, see Chapter 8, "Software Restriction Policies."

Countermeasure

Configure the Network access: Do not allow storage of credentials or .NET Passports for network authentication setting to Enabled.

Potential 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. 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.

Network access: Let Everyone permissions apply to anonymous users

This policy setting determines what additional permissions are granted for anonymous connections to the computer. If you enable this policy setting, anonymous users can enumerate the names of domain accounts and network shares and perform certain other activities. This capability is convenient, for example, when an administrator wants to grant access to users in a trusted domain that does not maintain a reciprocal trust.

By default, the token that is created for anonymous connections does not include the Everyone SID. Therefore, permissions that are assigned to the Everyone group do not apply to anonymous users. If you enable this policy setting, the Everyone SID is added to the token that is created for anonymous connections, and anonymous users will be able to access any resource for which the Everyone group has been assigned permissions.

The possible values for the Network access: Let Everyone permissions apply to anonymous users setting are:

• Enabled
• Disabled
• Not Defined

Vulnerability

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

Countermeasure

Configure the Network access: Let Everyone permissions apply to anonymous users setting to Disabled.
Potential Impact

None. This is the default configuration.

**Network access: Named Pipes that can be accessed anonymously**

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

The possible values for the **Network access: Named Pipes that can be accessed anonymously** setting are:

- A user-defined list of shares
- Not Defined

For this policy setting to take effect, you must also enable the **Network access: Restrict anonymous access to named pipes and shares** setting.

**Vulnerability**

You can restrict access over named pipes such as COMNAP and LOCATOR to help prevent unauthorized access to the network. The default list of named pipes and their purpose is provided in the following table.

**Table 5.1: Default Named Pipes That Are Accessible Anonymously**

<table>
<thead>
<tr>
<th>Named pipe</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMNAP</td>
<td>SNABase named pipe. Systems Network Architecture (SNA) is a collection of network protocols that were originally developed for IBM mainframe computers.</td>
</tr>
<tr>
<td>COMNODE</td>
<td>SNA Server named pipe.</td>
</tr>
<tr>
<td>SQL\QUERY</td>
<td>Default named pipe for SQL Server.</td>
</tr>
<tr>
<td>SPOOLSS</td>
<td>Named pipe for the Print Spooler service.</td>
</tr>
<tr>
<td>EPMAPPER</td>
<td>End Point Mapper named pipe.</td>
</tr>
<tr>
<td>LOCATOR</td>
<td>Remote Procedure Call Locator service named pipe.</td>
</tr>
<tr>
<td>TrkWks</td>
<td>Distributed Link Tracking Client named pipe.</td>
</tr>
<tr>
<td>TrkSvr</td>
<td>Distributed Link Tracking Server named pipe.</td>
</tr>
</tbody>
</table>

**Countermeasure**

Configure the **Network access: Named Pipes that can be accessed anonymously** setting to a null value (enable the setting but do not enter named pipes in the text box).

**Potential 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.

**Network access: Remotely accessible registry paths**

This policy setting determines which registry paths will be accessible when an application or process references the `WinReg` key to determine access permissions.

The possible values for the **Network access: Remotely accessible registry paths** setting are:

- A user-defined list of paths
- Not Defined

**Vulnerability**

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.

**Countermeasure**

Configure the **Network access: Remotely accessible registry paths** setting to a null value (enable the setting but do not enter any paths in the text box).

**Potential 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.

**Network access: Remotely accessible registry paths and sub-paths**

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.

The possible values for the **Network access: Remotely accessible registry paths and sub-paths** setting are:

- A user-defined list of paths
- Not Defined

**Vulnerability**

As stated earlier, 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.

Countermeasure

Configure the **Network access: Remotely accessible registry paths and sub-paths** setting to a null value (enable the setting but do not enter any paths in the text box).

Potential 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.

**Network access: Restrict anonymous access to Named Pipes and Shares**

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 registry key `HKLM\System\CurrentControlSet\Services\LanManServer\Parameters`. This registry value toggles null session shares on or off to control whether the server service restricts unauthenticated clients’ access to named resources.

The possible values for the **Network access: Restrict anonymous access to Named Pipes and Shares** setting are:

- Enabled
- Disabled
- Not Defined

Vulnerability

Null sessions are a weakness that can be exploited through shares (including the default shares) on computers in your environment.

Countermeasure

Configure the **Network access: Restrict anonymous access to Named Pipes and Shares** setting to **Enabled**.

Potential Impact

You can enable this policy setting to restrict null session access for unauthenticated users to all server pipes and shares except those that are listed in the **NullSessionPipes** and **NullSessionShares** entries.
**Network access: Shares that can be accessed anonymously**

This policy setting determines which network shares can be accessed by anonymous users.

The possible values for the **Network access: Shares that can be accessed anonymously** setting are:

- A user-defined list of shares
- Not Defined

**Vulnerability**

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.

**Countermeasure**

Configure the **Network access: Shares that can be accessed anonymously** setting to a null value.

**Potential Impact**

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

**Network access: Sharing and security model for local accounts**

This policy setting determines how network logons that use local accounts are authenticated. If you configure this policy setting to **Classic**, network logons that use local account credentials authenticate with those credentials. If you configure this policy setting to **Guest only**, network logons that use local accounts are automatically mapped to the Guest account. The **Classic** model provides precise control over access to resources, and allows you to grant different types of access to different users for the same resource. Conversely, the **Guest only** model treats all users equally as the Guest user account, and they all receive the same level of access to a given resource, which can be either Read Only or Modify.

The default configuration in stand-alone Windows XP Professional is **Guest only**. The default for Windows XP computers that are joined to a domain and Windows Server 2003 computers is **Classic**.

**Note**: This policy setting does not affect network logons that use domain accounts. Nor does this policy setting affect interactive logons that are performed remotely through services such as Telnet or Terminal Services.

When the computer is not joined to a domain, this policy setting also tailors the **Sharing** and **Security** tabs in Windows Explorer to correspond to the sharing and security model that is being used.

This setting has no effect on Windows 2000 computers.
The possible values for the **Network access: Sharing and security model for local accounts** setting are:

- **Classic**. Local users authenticate as themselves.
- **Guest only**. Local users authenticate as Guest.
- **Not Defined**

**Vulnerability**

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.

**Countermeasure**

For network servers, configure the **Network access: Sharing and security model for local accounts** setting to **Classic** – **local users authenticate as themselves**. On end-user computers, configure this policy setting to **Guest only** – **local users authenticate as guest**.

**Potential Impact**

None. This is the default configuration.

**Network security: Do not store LAN Manager hash value on next password change**

This policy setting determines whether LAN Manager can store hash values for the new password the next time the password is changed.

The possible values for the **Network security: Do not store LAN Manager hash value on next password change** setting are:

- **Enabled**
- **Disabled**
- **Not Defined**

**Vulnerability**

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.
Chapter 5: Security Options

Countermeasure

Configure the **Network security: Do not store LAN Manager hash value on next password change** setting to **Enabled**. Require all users to set new passwords the next time they log in to the domain so that LAN Manager hashes are removed.

Potential Impact

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

**Network security: Force logoff when logon hours expire**

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 server will be 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.

The possible values for the **Network security: Force logoff when logon hours expire** setting are:

- Enabled
- Disabled
- Not Defined

Vulnerability

If you disable this policy setting, a user could remain connected to the computer outside of their allotted logon hours.

Countermeasure

Configure the **Network security: Force logoff when logon hours expire** setting to **Enabled**. This policy setting does not apply to administrator accounts.

Potential Impact

When a user's logon time expires, SMB sessions will terminate. The user will be unable to log on to the computer until their next scheduled access time commences.

**Network security: LAN Manager authentication level**

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).
Chapter 5: Security Options 101

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).

**Vulnerability**

Windows 2000, Windows Server 2003, and Windows XP clients are configured by default to send LM and NTLM authentication responses (Windows 9x 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 9x 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 9x 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 legacy 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.

For more information about how to enable NTLMv2, see the Microsoft Knowledge Base article “How to enable NTLM 2 authentication,” which is located at http://support.microsoft.com/default.aspx?scid=239869. Microsoft Windows NT 4.0 requires Service Pack 4 (SP4) to support NTLMv2, and Windows 9x platforms need the Directory Service client installed to support NTLMv2.

**Countermeasure**

Configure the **Network security: LAN Manager Authentication Level** setting to **Send NTLMv2 responses only**. This level of authentication is strongly recommended by Microsoft and a number of independent organizations when all clients support NTLMv2.
Potential 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 computers along with Windows 2000, Windows XP, and Windows Server 2003 computers, refer to the Microsoft Knowledge Base article “Authentication Problems in Windows 2000 with NTLM 2 Levels Above 2 in a Windows NT 4.0 Domain” at http://support.microsoft.com/default.aspx?scid=305379.

Network security: LDAP client signing requirements

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

Vulnerability

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.

Countermeasure

Configure the Network Security: LDAP server signing requirements setting to Require signature.
Potential 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.

Network security: Minimum session security for NTLM SSP based (including secure RPC) clients

This policy setting allows a client computer to require the negotiation of message confidentiality (encryption), message integrity, 128-bit encryption, or NTLMv2 session security. These values are dependent on the LAN Manager Authentication Level policy setting value.

The possible values for the Network security: Minimum session security for NTLM SSP based (including secure RPC) clients setting are:

- **Require message confidentiality**. The connection will fail if encryption is not negotiated. Encryption converts data into a form that is not readable until decrypted.
- **Require message integrity**. 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**.

Vulnerability

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.

Countermeasure

Enable all four options that are available for the Network security: Minimum session security for NTLM SSP based (including secure RPC) clients policy setting.

Potential Impact

Client computers that are enforcing these settings will be unable to communicate with older servers that do not support them.
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers

This policy setting allows a server to require the negotiation of message confidentiality (encryption), message integrity, 128-bit encryption, or NTLMv2 session security. These values are dependent on the LAN Manager Authentication Level security setting value.

The possible values for the Network security: Minimum session security for NTLM SSP based (including secure RPC) servers setting are:

- **Require message confidentiality**. The connection will fail if encryption is not negotiated. Encryption converts data into a form that is not readable by anyone until decrypted.
- **Require message integrity**. 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**.

Vulnerability

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.

Countermeasure

Enable all four options that are available for the Network security: Minimum session security for NTLM SSP based (including secure RPC) servers policy.

Potential Impact

Older clients that do not support these security settings will be unable to communicate with the computer.

Recovery console: Allow automatic administrative logon

This policy setting determines whether the Administrator account password must be provided before access to the computer is granted. If you enable this setting, the Administrator account is automatically logged on to the computer at the Recovery Console; no password is required.
The possible values for the **Recovery console: Allow automatic administrative logon** setting are:

- Enabled
- Disabled
- Not Defined

**Vulnerability**

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 log on 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.

**Countermeasure**

Configure the **Recovery Console: Allow automatic administrative logon** setting to **Disabled**.

**Potential Impact**

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

**Recovery console: Allow floppy copy and access to all drives and all folders**

You can enable this policy setting to make 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**. Suppresses the prompt that typically displays before an existing file is overwritten.

The possible values for the **Recovery console: Allow floppy copy and access to all drives and all folders** setting are:

- Enabled
- Disabled
- Not Defined

**Vulnerability**

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

Configure the **Recovery Console: Allow floppy copy and access to drives and folders** setting to **Disabled**.

**Potential 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.

**Shutdown: Allow system to be shut down without having to log on**

This policy setting determines whether a computer can be shut down without having to log on to Windows. If you enable this policy setting, the **Shut Down** command is available on the Windows logon screen. If you disable this policy setting, the **Shut Down** option is removed from the Windows logon screen. This configuration requires users to be able to log on to the computer successfully and have the **Shut down the system** user right before they can perform a computer shutdown.

The possible values for the **Shutdown: Allow system to be shut down without having to log on** setting are:

- **Enabled**
- **Disabled**
- **Not Defined**

**Vulnerability**

Users who can access the console locally could shut down the computer.

Attackers could also walk to the local console and restart the server, which would cause a temporary DoS condition. Attackers could also shut down the server and leave all of its applications and services unavailable.

**Countermeasure**

Configure the **Allow system to be shut down without having to log on** setting to **Disabled**.

**Potential Impact**

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

**Shutdown: Clear virtual memory page file**

This policy setting determines whether the virtual memory page file is cleared when the computer is shut down. Virtual memory support uses a system page file to swap pages of memory to disk when they are not used. On a running computer, this page file is opened exclusively by the operating system, and it is well protected. However, computers that are configured to allow other operating systems to start might have to make sure that the system page file is wiped clean when the computer shuts down. This confirmation ensures that sensitive information from process memory that might be placed in the page file is not available to an unauthorized user who manages to directly access the page file after shutdown.
When you enable this policy setting, the system page file is cleared upon clean shutdown. Also, this policy setting will force the computer to clear the hibernation file Hiberfil.sys when hibernation is disabled on a portable computer.

The possible values for the **Shutdown: Clear virtual memory page file** setting are:

- Enabled
- Disabled
- Not Defined

**Vulnerability**

Important information that is kept in real memory may be written periodically to the page file to help Windows Server 2003 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.

**Countermeasure**

Configure the **Clear virtual memory page file when system shuts down** setting to **Enabled**. This configuration causes Windows Server 2003 to clear the page file when the computer is shut down. The amount of time that is required to complete this process depends on the size of the page file. It could be several minutes before the computer completely shuts down.

**Potential Impact**

It will take longer to shut down and restart the server, especially on servers with large paging files. For a server with 2 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.

**System cryptography: Force strong key protection for user keys stored on the computer**

This policy setting determines whether users can use private keys, such as their S/MIME key, without a password.

The possible values for the **System cryptography: Force strong key protection for user keys stored on the computer** setting are:

- User input is not required when new keys are stored and used
- User is prompted when the key is first used
- User must enter a password each time they use a key
- Not Defined
Vulnerability

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.

Countermeasure

Configure the System cryptography: Force strong key protection for user keys stored on the computer setting to User must enter a password each time they use a key.

Potential 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. At a minimum, this setting should be set to User is prompted when the key is first used.

System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing

This policy setting determines whether the TLS/SSL Security Provider will only support the strong cipher suite known as TLS_RSA_WITH_3DES_EDE_CBC_SHA, which means that the provider only supports the TLS protocol as a client and as a server, if applicable. It uses only the Triple Data Encryption Standard (DES) encryption algorithm for the TLS traffic encryption, only the Rivest-Shamir-Adleman (RSA) public key algorithm for the TLS key exchange and authentication, and only the Secure Hash Algorithm version 1 (SHA-1) hashing algorithm for the TLS hashing requirements.

When this setting is enabled, the Encrypting File System Service (EFS) supports only the Triple DES encryption algorithm for encrypting file data. By default, the Windows Server 2003 implementation of EFS uses the Advanced Encryption Standard (AES) with a 256-bit key. The Windows XP implementation uses DESX.

The possible values for the System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing setting are:

• Enabled
• Disabled
• Not Defined

Vulnerability

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.
Countermeasure
Configure the **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing** setting to **Enabled**.

Potential 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 will 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 Explorer to use TLS
1. On the Internet Explorer **Tools** menu, open the **Internet Options** dialog box.
2. Click the **Advanced** tab.
3. Select the **Use TLS 1.0** checkbox.

It is also possible to configure this policy setting through Group Policy or by using the Internet Explorer Administrators Kit.

**System objects: Default owner for objects created by members of the Administrators group**
This policy setting determines whether the **Administrators group** or an object creator is the default owner of any system objects that are created.

The possible values for the **System objects: Default owner for objects created by members of the Administrators group** setting are:

- Administrators group
- Object creator
- Not Defined

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

Countermeasure
Configure the **System objects: Default owner for objects created by members of the Administrators group** setting to **Object creator**.
Potential 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 will 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.

System objects: Require case insensitivity for non-Windows subsystems

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 Portable Operating System Interface for UNIX (POSIX). If you enable this setting, case insensitivity is enforced for all directory objects, symbolic links, and IO as well as file objects. If you disable this setting, the Win32 subsystem does not become case-sensitive.

The possible values for the System objects: Require case insensitivity for non-Windows subsystems setting are:

- Enabled
- Disabled
- Not Defined

Vulnerability

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.

Countermeasure

Configure the System objects: Require case insensitivity for non-Windows subsystems setting to Enabled.

Potential Impact

All subsystems will be forced to observe case insensitivity. This configuration may confuse users who are familiar with one of the UNIX-based operating systems that are case-sensitive.
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)

This policy setting determines the strength of the default DACL for objects. Windows maintains a global list of shared computer resources (such as MS-DOS device names, mutexes, and semaphores) so that objects can be located and shared among processes.

The possible values for the System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links) setting are:

- Enabled
- Disabled
- Not Defined

Vulnerability

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.

Countermeasure

Configure the System objects: Strengthen default permissions of global system objects (for example, Symbolic Links) setting to Enabled.

Potential Impact

None. This is the default configuration.

System settings: Optional subsystems

This policy setting determines which subsystems support your applications. You can use this security setting to specify as many subsystems as your environment demands.

The possible values for the System settings: Optional subsystems setting are:

- A user-defined list of subsystems
- Not Defined

Vulnerability

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.
Countermeasure

Configure the System settings: Optional subsystems setting to a null value. The default value is POSIX.

Potential 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.


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. This security setting 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 Authenticode®-signed software to run, based on the digital certificate that is associated with the software. For certificate rules to work in software restriction policies, you must enable this security setting.

The possible values for the System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies setting are:

- Enabled
- Disabled
- Not Defined

Vulnerability

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

Countermeasure


Potential 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.
More Information

The following links provide additional information about security options in Windows Server 2003 and Windows XP.


• For information about default COM access restrictions in Windows Server 2003 with SP1, see the "DCOM Security Enhancements" section in the "Changes to Functionality in Microsoft Windows Server 2003 Service Pack 1" guide at www.microsoft.com/technet/prodtechnol/windowsserver2003/library/BookofSP1/.

• For more information about how to enable NTLMv2, see the Microsoft Knowledge Base article "How to enable NTLM 2 authentication" at http://support.microsoft.com/default.aspx?scid=239869.

• For more information about how to ensure that more secure LAN Manager Authentication Level settings work in networks with a mix of Windows 2000 and Windows NT® 4.0 computers, see the Microsoft Knowledge Base article "Authentication Problems in Windows 2000 with NTLM 2 Levels Above 2 in a Windows NT 4.0 Domain" at http://support.microsoft.com/?scid=305379.

• For more information about LAN Manager compatibility levels, see the Microsoft Knowledge Base article "Client, service, and program incompatibilities that may occur when you modify security settings and user rights assignments" at http://support.microsoft.com/?scid=823659.

• For more information about NTLMv2 authentication, see the Microsoft Knowledge Base article "How to Enable NTLM 2 Authentication" at http://support.microsoft.com/?scid=239869.

• For more information about how to restore default security settings locally, see Microsoft Knowledge Base article "How to Reset Security Settings Back to the Defaults" at http://support.microsoft.com/?scid=313222.

• For more information about how to restore default security settings in the built-in domain Group Policy objects, see Microsoft Knowledge Base Article "How to Reset User Rights in the Default Domain Group Policy in Windows Server 2003" at http://support.microsoft.com/?scid=324800.
Event Log

The event log records events on the computer, and the Security log records audit events. The event log container of Group Policy is used to define the attributes that are related to the Application, Security, and System event logs, such as maximum log size, access rights for each log, and retention settings and methods. The Microsoft® Excel® workbook “Windows Default Security and Services Configuration,” which is included with this guide, documents the default event log settings.

Event Log Settings

You can configure the event log settings in the following location within the Group Policy Object Editor:

Computer Configuration\Windows Settings\Security Settings\Event Logs\Settings for Event Logs

Maximum event log size

This policy setting specifies the maximum size of the Application, Security, and System event logs. Although the user interfaces (UIs) of both the Group Policy Object Editor and the Microsoft Management Console (MMC) Event Viewer snap-in allow you to enter values as large as four GB, certain factors make the effective maximum size for these logs much smaller.

The Event Log service uses memory-mapped files, and it runs as one of the services under the Services.exe process as Eventlog.dll. When files are loaded in this way, the entire file is loaded into the computer's memory. All of the current versions of Microsoft Windows® have an architectural limitation with regard to memory-mapped files: no process can have more than one GB of memory-mapped files in total. This limitation means that all of the services that run under the Services.exe process must share the one GB pool. The memory is assigned in contiguous 64 KB portions, and if the computer cannot assign additional memory to expand memory-mapped files, problems will occur.

For the Event Log service, the use of memory-mapped files means that regardless of the amount of memory that the Maximum event log size setting specifies, log events may no longer be recorded in the log when the computer has no more memory available for the memory-mapped file. Error messages will not be displayed; the events will simply not appear in the event log, or they may overwrite other events that had been recorded previously. Fragmentation of the log files within memory has also been shown to lead to significant performance problems on busy computers.
Because of these limitations—even though the theoretical limit for memory-mapped files suggests otherwise and the Event Viewer and Group Policy Object Editor UIs allow you to specify as much as four GB per log—Microsoft has verified that the practical limit is approximately 300 MB on most servers—that is, 300 MB for all of the event logs combined. On Microsoft Windows XP, member servers, and stand-alone servers, the combined size of the Application, Security, and System event logs should not exceed 300 MB. On domain controllers, the combined size of these three logs plus the Active Directory® directory service, DNS, and Replication logs should not exceed 300 MB.

These limitations have caused problems for some Microsoft customers, but the only way to remove the limitations requires fundamental changes to the way system events are recorded. Microsoft is rewriting the event log system to resolve these problems in the next version of Windows.

Although there is no simple equation to determine the best log size for a particular server, you can calculate a reasonable size. The average event takes up about 500 bytes within each log, and the log file sizes must be a multiple of 64 KB. If you can estimate the average number of events that are generated each day for each type of log in your organization, you can determine a good size for each type of log file.

For example, if your file server generates 5,000 events per day in its Security log and you want to ensure that you have at least 4 weeks of data available at all times, then you would want to configure the size of that log to about 70 MB. (500 bytes * 5000 events/day * 28 days = 70,000,000 bytes.) Then, check the servers occasionally over the following four weeks to verify your calculations and that the logs retain enough events for your needs. Event log size and log wrapping should be defined to match the business and security requirements you determined when you designed your organization’s security plan.

The possible values for the Maximum event log size setting are:

- A user-defined value in kilobytes between 64 and 4,194,240. However, it must be a multiple of 64.

**Vulnerability**

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.

**Countermeasure**

You should enable sensible log size policies for all computers in your organization so that legitimate users can be held accountable for their actions, unauthorized activity can be detected and tracked, and computer problems can be detected and diagnosed.

**Potential 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.

**Prevent local guests group from accessing event logs**

This policy setting determines whether guests can access the Application, Security, and System event logs.

The possible values for the Prevent local guests group from accessing event logs setting are:

- Enabled
- Disabled
- Not Defined

**Note:** This policy setting does not appear in the Local Computer Policy object.

This policy setting only affects computers that run Windows 2000 and subsequent versions of Windows.

**Vulnerability**

An attacker who has successfully logged onto a computer with guest privileges could learn important information about the computer if they were able to view the event logs. The attacker could then use this information to implement additional exploits.

**Countermeasure**

Enable the Prevent local guests group from accessing event logs setting for the policies of all three event logs.

**Potential Impact**

None. This is the default configuration.

**Retain event logs**

This policy setting determines the number of days of event log data to retain for the Application, Security, and System logs if the retention method that is specified for the log is By Days. Configure this setting only if you archive the log at scheduled intervals and you make sure that the maximum log size is large enough to accommodate the interval.
The possible values for the **Retain event logs** setting are:

- A user-defined number in days between 1 and 365
- Not Defined

**Note:** This policy setting does not appear in the Local Computer Policy object.

A user must be assigned the **Manage auditing and security log** user right to access the Security log.

**Vulnerability**

If you archive the log at scheduled intervals:

1. Open the **Properties** dialog box for this policy.
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.

**Countermeasure**

Configure the **Retain event logs** setting for the policies of all three event logs to **Not Defined**.

**Potential Impact**

None. This is the default configuration.

**Retention method for event log**

This policy setting determines the wrapping method for the Application, Security, and System logs.

If you do not want to archive the Application log:

1. Open the **Properties** dialog box for this policy.
2. Select the **Define this policy setting** check box.
3. Click **Overwrite events as needed**.

If you want to archive the log at scheduled intervals:

1. Open the **Properties** dialog box for this policy.
2. Select the **Define this policy setting** check box.
3. Click **Overwrite events by days**.
4. Specify the appropriate number of days in the **Retain application log** setting. Ensure that the maximum log size is large enough to accommodate the interval.

If you must retain all the events in the log:

1. Open the **Properties** dialog box for this policy.
2. Select the **Define this policy setting** check box.
3. Click **Do not overwrite events (clear log manually)**.

This option requires that the log be cleared manually. In this configuration, new events are discarded when the maximum log size is reached.
The possible values for the **Retention method for event log** setting are:

- Overwrite events by days
- Overwrite events as needed
- Do not overwrite events (clear log manually)
- Not defined

**Note:** This policy setting does not appear in the Local Computer Policy object.

**Vulnerability**

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 Chapter 5, "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.

**Countermeasure**

Configure the retention method for all three event logs to the option **Overwrite events as needed**. Some resources recommend that you configure this setting to **Manual**; however, the administrative burden that this setting imposes is too great for most organizations.

Ideally, all significant events will be sent to a monitoring server that uses MOM or some other automated monitoring tool.

**Potential 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.
Delegating Access to the Event Logs

In Microsoft Windows Server™ 2003, it is possible to customize the permissions on each event log on a computer. This capability was not available in previous versions of Windows. Some organizations may want to grant read-only access to one or more of the System event logs to some members of the IT team. The access control list (ACL) is stored as a Security Descriptor Definition Language (SDDL) string, in a REG_SZ value called "CustomSD" for each event log in the registry, as in the following example:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\CustomSD
Create a REG_SZ registry value
O:BAG:SYD:(D;;0xf0007;;;AN)(D;;0xf0007;;;BG)
(A;;0xf0007;;;SY)(A;;0x7;;;BA)(A;;0x5;;;SO)(A;;0x1;;;IU)(A;;0x1;;;SU)
(A;;0x1;;;S-1-5-3)(A;;0x2;;;LS)(A;;0x2;;;NS)
```

If you edit this value and restart the computer, the new setting will take effect.

**Caution:** Be careful when you edit the registry values, because there is no "undo" function in the Registry Editor tool. If you make a mistake, you will have to correct it manually. Also, you could accidentally configure the ACLs on an event log in such a way that no one could access it. Be certain that you fully understand SDDL and the default permissions that are placed on each event log before you proceed. Also, be certain to test any changes thoroughly before you implement them in a production environment.


More Information

The following links provide additional information about event logging in Windows Server 2003 and Windows XP.


System Services

System services are described differently than the other settings in this guide because the vulnerability, countermeasure, and potential impact statements are almost identical for all services.

When you first install Microsoft® Windows Server™ 2003 or Microsoft Windows® XP, some services are installed and configured to run by default when the computer starts. There are fewer default services than there were in Windows 2000 Server, and for Windows Server 2003 the specific services will vary in accordance with the role that is assigned to each server. You may not need all of the default services in your environment, and you should disable any unneeded services to enhance security.

This chapter will help identify the function and purpose of each service, and explain which services were left enabled in Windows Server 2003 and Windows XP to ensure application compatibility, client compatibility, or to facilitate computer system management. The Microsoft Excel® workbook "Windows Default Security and Services Configuration" (included with the downloadable version of this guide) documents the default system service settings.
Threats and Countermeasures

Services Overview

A service must log on to access resources and objects in the operating system, and most services are not designed to have their default logon account changed. If you change the default account, it is likely that the service will fail. If you select an account that does not have permission to log on as a service, the Microsoft Management Console (MMC) Services snap-in automatically grants that account the ability to log on as a service on the computer. However, this automatic configuration does not guarantee that the service will start. Windows Server 2003 includes three built-in local accounts that are used as the logon accounts for various system services:

- **Local System account.** The Local System account is a powerful account that has full access to the computer and acts as the computer on the network. If a service uses the Local System account to log on to a domain controller, that service has access to the entire domain. Some services are configured by default to use the Local System account, and this should not be changed. The Local System account does not have a user-accessible password.

- **Local Service account.** The Local Service account is a special, built-in account that is similar to an authenticated user account. It has the same level of access to resources and objects as members of the Users group. This limited access helps safeguard your computer if individual services or processes are compromised. Services that use the Local Service account access network resources as a null session with anonymous credentials. The name of this account is NT AUTHORITY\Local Service, and it does not have a user-accessible password.

- **Network Service account.** The Network Service account is also a special, built-in account that is similar to an authenticated user account. Like the Local Service account, it has the same level of access to resources and objects as members of the Users group, which helps safeguard your computer. Services that use the Network Service account access network resources with the credentials of the computer account. The name of the account is NT AUTHORITY\Network Service, and it does not have a user-accessible password.

**Important:** If you change the default service settings, key services may not run correctly. It is especially important to use caution if you change the Startup type and Log on as settings of services that are configured to start automatically.

You can configure the system services settings in the following location within the Group Policy Object Editor:

```
Computer Configuration\Windows Settings\Security Settings\System Services\
```

Vulnerability

Any service or application is a potential point of attack. Therefore, you should disable or remove any unneeded services or executable files in your environment. There are additional optional services available in Windows Server 2003, such as Certificate Services, that are not installed during a default installation of the operating system.

You can add these optional services to an existing computer through Add/Remove Programs in Control Panel or the Windows Server 2003 Configure Your Server Wizard. You can also create a customized automated installation of Windows Server 2003. In the Member Server Baseline Policy (MSBP) that is described in the Windows Server 2003 Security Guide (available at http://go.microsoft.com/fwlink/?LinkId=14845), these optional services and all unnecessary services are disabled.
Important: If you enable additional services, they may depend on other services. Add all of the services that are needed for a specific server role to the policy for the server role that it performs in your organization.

**Countermeasure**

Disable all unnecessary services.

For each system service, you can assign a service state through Group Policy. The possible values for these Group Policy settings are:

- Automatic
- Manual
- Disabled
- Not Defined

Another way to manage service security is to configure an access control list (ACL) for each service with a user-defined list of accounts. This method provides a way to control launching of the service and access to the running service.

**Potential Impact**

If some services (such as the Security Accounts Manager) are disabled, you will not be able to restart the computer. If other critical services are disabled, the computer may not be able to authenticate with domain controllers. If you wish to disable some system services, you should test the changed settings on non-production computers before you change them in a production environment.
**Do Not Set Permissions on Service Objects**

There are graphical user interface (GUI)–based tools that you can use to edit services. However, previous versions of these tools that were included with earlier versions of the Windows operating system (before Windows Server 2003) automatically apply permissions to each service when you configure any of the properties of a service. Tools such as the Group Policy Object Editor and the MMC Security Templates snap-in use the Security Configuration Editor DLL to apply these permissions.

For example, when you use the MMC Security Templates snap-in to configure the startup state of a service in Windows XP, the following dialog box will display:

![Figure 7.1 Services Security Dialog Box](image)

Regardless of whether you click **OK** or **Cancel**, the permissions will be applied to the service that is being configured. Unfortunately, the permissions that this dialog box proposes do not match the default permissions for most services that are included with Windows. In fact, the permissions will cause a variety of problems for many services. Microsoft recommends that you not alter the permissions on services that are included with Windows XP or Windows Server 2003 because the default permissions are already quite restrictive.
This functionality changed in Windows Server 2003, and its version of the Security Configuration Editor DLL does not force you to configure permissions when you edit the properties of a service. You have several different options to deal with this challenging situation:

- Use the Security Configuration Wizard, an optional Windows component that is included with Windows Server 2003 Service Pack 1 (SP1). Microsoft recommends this approach when you need to configure services and network port filters for various Windows Server 2003 server roles.
- Run the MMC Security Template snap-in and Group Policy Object Editor on a server that runs Windows Server 2003 with SP1. Microsoft recommends this approach when you need to configure services for security templates or Group Policies that will be applied to Windows XP.
- Use a text editor such as Notepad to edit the security templates or Group Policies on a computer that runs Windows XP Professional. This method is the least desirable, but some customers may have no choice. Detailed instructions are provided in the following section.

### Manually Editing Security Templates

Although you can use a text editor such as Notepad to manually edit them, security templates, are complex files. Security templates that are created with an incorrectly defined template specification can make a computer unbootable. Although most types of mistakes will not cause such a serious problem, you must be patient and pay attention to detail if you need to manually edit security templates.

When you use one of the GUI–based tools to configure services in a security template, the configuration information is stored in the “Service General Setting” section of the file. The following sample text is from a security template in which the Alerter, ClipBook, and Computer Browser services have had their startup state configured to Disabled and the DHCP Client service has had its startup state configured to Automatic.

```
[Service General Setting]
Alerter,4,"D:AR(A;;CCDCLCSWRPWPDPDTCRCRSRCDRCDWRCDWO;;;Y)(A;;CCLCSWLOCRCDRCWDWO;;;IU)S:(AU;FA;CCDCLCSWRPWPDPDTCRCRSRCDRCDWRCDWO;;;WD)"
ClipSrv,4,"D:AR(A;;CCDCLCSWRPWPDPDTCRCRSRCDRCDWRCDWO;;;;Y)(A;;CCLCSWLOCRCDRCWDWO;;;IU)S:(AU;FA;CCDCLCSWRPWPDPDTCRCRSRCDRCDWRCDWO;;;WD)"
Browser,4,"D:AR(A;;CCDCLCSWRPWPDPDTCRCRSRCDRCDWRCDWO;;;;Y)(A;;CCLCSWLOCRCDRCWDWO;;;IU)S:(AU;FA;CCDCLCSWRPWPDPDTCRCRSRCDRCDWRCDWO;;;WD)"
Dhcp,2,"D:AR(A;;CCDCLCSWRPWPDPDTCRCRSRCDRCDWRCDWO;;;;Y)(A;;CCLCSWLOCRCDRCWDWO;;;IU)S:(AU;FA;CCDCLCSWRPWPDPDTCRCRSRCDRCDWRCDWO;;;WD)"
```

The format for each entry includes three comma-separated fields.

- The first field specifies the service name. For example, ClipSrv indicates the ClipBook service.
- The second field defines the startup state:
  - 4 specifies Disabled
  - 3 specifies Manual
  - 2 specifies Automatic
• The third field defines the permissions for the service object in Security Descriptor Definition Language (SDDL).

You do not have to understand the details of SDDL to use the Security Configuration Wizard. You can find more information about SDDL in the article "Security Descriptor Definition Language" on MSDN® at http://msdn.microsoft.com/library/en-us/secauthz/security/security_descriptor_definition_language.asp.

To resolve potential problems with permissions on the service objects, remove the SDDL string in the third field but leave the pair of double-quotiation marks. The following example shows the correct text for the four referenced services:

```
[Service General Setting]
Alerter,4,""
ClipSrv,4,""
Browser,4,""
Dhcp,2,""
```

After you remove the SDDL information from all of the services in the security template, save the file. You can than apply the security template through any of the typical methods. Of course, it is extremely important that you test security templates thoroughly before you apply them to production computers.
Descriptions of System Services

The following subsections describe the Windows Server 2003 and Windows XP services in alphabetical order. Services that are installed by default are included as well as additional services that can be added to the computer.

Note: If a service is not started, other services that depend on that service will also fail to start. Therefore, if you change the status of one service you may affect other seemingly unrelated services. Such dependencies exist for all of the services that are described in this section. To check the dependencies for a service, click the Dependencies tab of the service's properties dialog in the MMC Services snap-in.

Alerter

The Alerter service notifies selected users and computers of administrative alerts. You can use this service to send alert messages to specified users that are connected on your network.

Alert messages warn users about security, access, and user session problems. Alert messages are sent from a server to a client computer, and the Messenger service must be running on the client computer for the user to receive alert messages. (The Messenger service is disabled by default in Windows XP and Windows Server 2003 so that malicious users cannot send false notifications.)

If the Alerter service is turned off, applications that use the NetAlertRaise or NetAlertRaiseEx application programming interfaces (APIs) will be unable to notify a user or computer—by means of a message box that the Messenger service displays—that the administrative alert took place. For example, many uninterruptible power supply (UPS) management tools use the Alerter service to notify administrators of significant events that are related to the UPS. If you want to use this service, you should configure its startup state to Automatic so that external components can use it when needed.

Application Experience Lookup Service

The Application Experience Lookup Service (AELookupSvc) is a part of the Application Compatibility Administrator. It processes application compatibility lookup requests for applications as they are launched, provides support for Windows Server 2003 computers on a domain, reports on compatibility issues, and automatically applies software updates to programs.

The Application Experience Lookup Service must be active for application compatibility software updates be applied. You cannot customize this service; the operating system uses it internally. This service does not use any network, Internet, or Active Directory® directory service resources.

If you disable the Application Experience Lookup Service, the service will continue to run but no calls will be made to the service. You cannot stop the actual process.

Application Layer Gateway Service

The Application Layer Gateway Service is a subcomponent of the Windows networking subsystem. It provides support for plug-ins that allow network protocols to pass through the firewall and work behind Internet connection sharing. Application Layer Gateway (ALG) plug-ins can open ports and change data that is embedded in packets, such as ports and IP addresses. File Transfer Protocol (FTP) is the only network protocol that has

The ALG FTP plug-in is designed to support active FTP sessions through the Network Address Translation (NAT) engine that is included with Windows. To do this, the ALG FTP plug-in redirects all traffic that passes through the NAT and that is destined for port 21 to a private listening port in the 3000-5000 range on the loopback adapter. The ALG FTP plug-in then monitors/updates traffic on the FTP control channel so that the FTP plug-in can plumb port mappings through the NAT for the FTP data channels. The FTP plug-in will also update ports in the FTP control channel stream.

If the Application Layer Gateway Service stops, network connectivity for the referenced protocols will be unavailable and adversely affect the network. For example, if you disable this service the Windows Messenger and MSN® Messenger instant messaging applications will fail.

**Application Management**

The Application Management service provides software installation services such as Assign, Publish, and Remove. It processes requests to enumerate, install, and remove applications that are deployed through an organization’s network. When you click Add in Add/Remove Programs in Control Panel on a domain-joined computer, the program calls this service to retrieve the list of your deployed applications. The service is also called when you use Add/Remove Programs to install or remove an application. It is also called when a component (such as the shell or COM) makes an install request for an application to handle a file extension, Component Object Model (COM) class, or ProgID that is not present on the computer. The service is started by the first call that is made to it, and it does not terminate after it is started.

**Note:** For more information about COM, COM classes, or ProgIDs, see the Software Development Kit (SDK) information in the MSDN Library on the Windows Resource Kits - Web Resources page at www.microsoft.com/windows/reskits/webresources.

If the Application Management service stops or if you disable it, users will be unable to install, remove, or enumerate applications that are deployed in Active Directory through Microsoft IntelliMirror® management technologies. If you disable this service, it will not retrieve deployed application information and this information will not appear in the Add New Programs section of Add/Remove Programs in Control Panel. The Add programs from your network dialog box will display the following message:

No programs are available on the network.

You cannot stop this service after it is started without restarting the computer. If you do not require this service and do not want it to start, you must disable it.

**ASP .NET State Service**

The ASP .NET State Service provides support for out-of-process session states for ASP.NET. ASP.NET has a concept of session state—a list of values that are associated with the client session is accessible from ASP.NET pages through the Session setting. Three options are provided to store the session data: in process, Microsoft SQL Server™ database, and out-of-process session state server.

The ASP.NET State Service stores session data out-of-process. The service communicates with ASP.NET, which runs on the Web server using sockets. If this service stops or if you disable it, no out-of-process requests will be processed. The executable code for this service is installed by default, but the service itself is disabled until you manually change its startup type to Automatic or Manual.
Automatic Updates

The Automatic Updates service enables the download and installation of security updates for Windows and Office. It automatically provides Windows computers with the latest updates, drivers and enhancements. You no longer need to manually search for security updates and information; the operating system delivers them directly to your computer. The operating system recognizes when you are online and uses your Internet connection to search for applicable updates from the Windows Update service. Depending on your configuration settings, the service will either notify you before download, before installation, or the service will automatically install updates for you.

You can turn off the Automatic Update feature through the Systems setting in Control Panel. Alternatively, you can right-click My Computer and then click Properties.

You can also use the MMC Group Policy Object Editor snap-in to configure an intranet server that is configured with Windows Server Update Services to host updates from the Microsoft Update sites. This setting lets you specify a server on your network to function as an internal update service. The Automatic Updates client will search this service for updates that apply to the computers on your network.

Note: For more information about Windows Server Update Services, see the Windows Server Update Services Web site at http://go.microsoft.com/fwlink/?LinkId=21133.

If the Automatic Updates service stops or if you disable it, updates will not be automatically downloaded to the computer automatically. You will need to search for, download, and install applicable fixes through the Windows Update Web site at http://update.microsoft.com.

Background Intelligent Transfer Service (BITS)

The Background Intelligent Transfer Service is a background file transfer mechanism and queue manager. BITS transfers files asynchronously between a client and an HTTP server. By default, requests to BITS are submitted and the files are transferred through otherwise idle network bandwidth so that other network-related activities, such as browsing, are not affected.

BITS suspends the transfer if a connection is lost or if the user logs off. The BITS connection is persistent, and transfers information while the user is logged off, across network disconnects, and during computer restarts. When the user logs on, BITS resumes the user's transfer job.

BITS uses a queue to manage file transfers. You can prioritize transfer jobs within the queue and specify whether the files are transferred in the foreground or background. Background transfers are optimized by BITS, which increases and decreases (or throttles) the rate of transfer based on the amount of idle network bandwidth that is available. If a network application begins to consume more bandwidth, BITS decreases its transfer rate to preserve the user's interactive experience.

BITS provides one foreground and three background priority levels that you can use to prioritize transfer jobs. Higher priority jobs pre-empt lower priority jobs. Jobs at the same priority level share transfer time and round-robin scheduling prevents blockage of the transfer queue by a large job. Lower priority jobs do not receive transfer time until all higher priority jobs are complete or in an error state.

BITS is set to start manually on both Windows Server 2003 and Windows XP. It is started on demand when the first job is submitted. When all outstanding jobs are completed, BITS stops.
If **BITS** stops, features such as Automatic Update will be unable to automatically download programs and other information. This functionality means that the computer will also be unable to receive automatic updates from the organization’s Software Update Services server if one has been configured through Group Policy. If you disable this service, any services that explicitly depend on it will fail to transfer files unless they have a fail-safe mechanism to transfer files directly through other methods, such as Internet Explorer.

**Certificate Services**

The **Certificate Services** service functions as part of the core operating system to enable a business to act as its own certificate authority (CA) and issue and manage digital certificates for applications such as Secure/Multipurpose Internet Mail Extensions (S/MIME), Secure Sockets Layer (SSL), Encrypting File System (EFS), IP Security (IPsec), and smart card logon. Windows Server 2003 supports multiple levels of a CA hierarchy and cross-certified trust network, including offline and online CAs.

**Certificate Services** is not installed by default. Administrators must install it through Add/Remove Programs in Control Panel. If **Certificate Services** stops or if you disable it after installation, certificate requests will not be accepted and certificate revocation lists (CRLs) and delta CRLs will not be published. If the service stops long enough for CRLs to expire, existing certificates will fail to validate.

**Client Service for NetWare**

Servers with the **Client Service for NetWare** service installed provide access to file and print resources on NetWare networks for interactively logged-on users. With **Client Service for NetWare**, you can access file and print resources on Netware servers that run Novell Directory Services (NDS) or bindery security (NetWare versions 3.x or 4.x) from your computer.

**Client Service for NetWare** does not support the IP protocol and therefore cannot be used to interoperate with NetWare 5.x in an IP-only environment. To provide this capability, you must load the Internetwork Packet Exchange (IPX) protocol on the NetWare 5.x server or use a redirector that is compatible with Netware Core Protocol (NCP) and supports native IP.

If the **Client Service for NetWare** service stops or if you disable it, you will lose access to file and print resources on NetWare networks unless you install the Novell Client for NetWare. This service is not installed or enabled by default.

**ClipBook**

The **ClipBook** service enables the ClipBook Viewer to create and share pages of data for review by remote users. This service depends on the Network Dynamic Data Exchange (NetDDE) service to create the actual file shares that other computers can connect to. The ClipBook application and service allow you to create the pages of data to share.

The **ClipBook** service is installed by default, but its startup state is configured to **Disabled**. When this service stops, the ClipBook Viewer will not be able to share information with remote computers. Clipbrd.exe can still be used to view the local Clipboard, which is where data is stored when a user highlights text and either clicks **Copy** from the **Edit** menu or presses CTRL+C on the keyboard.
**Cluster Service**

The **Cluster Service** controls server cluster operations and manages the cluster database. A cluster is a collection of independent computers that work together to provide load balancing and failover support. Cluster-aware applications such as Microsoft Exchange Server and Microsoft SQL Server use the cluster to present a single virtual computer to users. The cluster software spreads data and computation tasks among the nodes of the cluster. When a node fails, other nodes provide the services and data that were formerly provided by the missing node. When a node is added or repaired, the cluster software migrates some data and computation tasks to that node.

There are two different types of cluster solutions for the Windows platform that support different application styles: server clusters and Network Load Balancing (NLB) clusters. Server clusters provide a highly available environment for applications that must run reliably for long periods of time (such as databases or file servers), and provide failover support with tightly integrated cluster management. NLB clusters provide a highly available and highly scalable environment for other types of applications such as front-end Web servers, and load balance client requests among a set of identical servers.

The **Cluster Service** provides support for server clusters. It is the essential software component that controls all aspects of the cluster operation and manages the cluster database. Each node in a cluster runs one instance of the **Cluster Service**.

Windows Server 2003 supports up to eight-node server clusters in both the Enterprise Server and Datacenter Server editions of Windows. However, a cluster can only consist of nodes that run one Windows edition or the other; different editions cannot run within a single cluster.

Server clusters can have one of three different configurations:

- **Single node.** These server clusters can be configured with or without external cluster storage devices. For single node clusters without an external cluster storage device, the local disk is configured as the cluster storage device. Use single node configurations to develop cluster-aware applications or use them in production to provide local health monitoring and restart capabilities to applications.

- **Single quorum device.** These server clusters have two or more nodes and are configured so that every node is attached to one or more cluster storage devices. The cluster configuration data is stored on a single cluster storage device, which is known as the quorum disk.

- **Majority node set.** These server clusters have two or more nodes in which the nodes may or may not be attached to one or more cluster storage devices. The cluster configuration data is stored on multiple disks across the cluster and the **Cluster Service** ensures that this data is kept consistent across the different disks.

The **Cluster Service** is not installed or enabled by default. If the **Cluster Service** stops after it is installed, clusters will be unavailable. For additional information about how to configure security for Windows clusters, review the relevant links in the “More Information” section at the end of this chapter.

**COM+ Event System**

The **COM+ Event System** service provides automatic event distribution to COM components that subscribe to it. COM+ events extend the COM+ programming model to support late-bound events or method calls between the publisher or subscriber and the event system. The event system notifies event consumers as information becomes available, and does not repeatedly poll the server.
The COM+ Event System service handles most of the event semantics for the publisher and subscriber. Publishers offer to publish event types, and subscribers request event types from specific publishers. Subscriptions are maintained outside the publisher and subscriber and retrieved when needed, which simplifies the programming model for both. The subscriber does not need to contain the logic to build subscriptions—it is possible to build a subscriber as easily as a COM component. The life cycle of the subscription is separate from that of either the publisher or the subscriber. You can build subscriptions before either the subscriber or publisher are made active. This service is installed by default, but is not started until an application requests its services. When COM+ Event System stops, the System Event Notification service will close and will not be able to provide logon and logoff notifications. The Volume Shadow Copy service, which is needed for Windows Backup and backup applications that rely upon the Windows Backup API, requires this service.

COM+ System Application

The COM+ System Application service manages the configuration and tracking of COM+-based components. If this service stops, most COM+-based components will not function properly. The Volume Shadow Copy service, which is needed for Windows Backup and backup applications that rely upon the Windows Backup API, requires this service. This service is installed and enabled by default.

Computer Browser

The Computer Browser service maintains an up-to-date list of computers on your network and supplies the list to programs that request it. The Computer Browser service is used by Windows-based computers that need to view network domains and resources. Computers that are designated as browsers maintain browse lists, which contain all shared resources that are used on the network. Earlier versions of Windows applications, such as My Network Places, the NET VIEW command, and Windows NT® Explorer, all require browsing capability. For example, if you open My Network Places on a Windows 95–based computer, a computer that is designated as a browser generates the list of domains and computers that displays.

There are several different roles a computer might perform in a browsing environment. Under some conditions, such as failure or shutdown of a computer that is designated for a specific browser role, browsers or potential browsers may change to a different operational role.

The Computer Browser service is enabled and started by default. If it stops, the browser list will not be updated or maintained.

Cryptographic Services

The Cryptographic Services service provides key-management services for your computer. Cryptographic Services is actually comprised of three different management services:

- Catalog Database Service. This service adds, removes, and looks up catalog files, which are used to sign all the files in the operating system. Windows File Protection (WFP), Driver Signing, and setup use this service to verify signed files. You cannot stop this service during setup. If the service stops after setup, it will be started by demand.
• **Protected Root Service.** This service adds and removes Trusted Root Certification Authority certificates. The service displays a service message box with the certificate’s name and thumbprint. If you click **OK**, the certificate is added or removed from your current list of trusted root authorities. Only Local System accounts have write-access to the list. If this service stops, the current user will not be able to add or remove Trusted Root Certificate Authority certificates.

• **Key Service.** This service allows administrators to enroll for certificates on behalf of the local computer account. The service provides several functions that are required for enrollment: enumeration of available certification authorities, enumeration of available computer templates, the ability to create and submit a certificate request in the local computer context, and so on. Only administrators may enroll on behalf of the local computer account. The Key Service also allows administrators to remotely install Personal Information Exchange (PFX) files on your computer. If this service stops, auto enrollment will not be able to automatically acquire the default set of computer certificates.

The **Cryptographic Services** service is enabled and started automatically by default. If it stops, the management services that are referenced in the preceding paragraphs will not function properly.

**DCOM Server Process Launcher**

In earlier versions of Windows, the Remote Procedure Call (RPC) service (RPCSS) ran as Local System. To reduce the attack surface of Windows and provide defense in depth, the RPC service functionality was split into two services in Windows XP Service Pack 2 and Windows Server 2003 Service Pack 1.

The RPCSS service retains all of the original functionality that did not require Local System privileges, and it now runs under the Network Service account. The **DCOM Server Process Launcher** (DCOMLaunch) service incorporates the functions of the old RPC service that required Local System privileges; it runs under the Local System account. This service is enabled and started by default.

If the **DCOM Server Process Launcher** service stops, remote procedure calls and DCOM requests on the local computer will not function properly. In particular, the Windows Firewall service will fail if this service stops.

**DHCP Client**

The **DHCP Client** service manages network configuration. It registers and updates IP addresses and DNS names for your computer. You do not have to manually change the IP settings for a client computer, such as a laptop, that connects from different locations throughout the network. The client computer is automatically given a new IP address, regardless of the subnet it reconnects to (if a DHCP server is accessible from the subnets). There is no need to manually configure settings for DNS or WINS. The DHCP server can provide these settings to the client if the DHCP server is configured to issue such information. To enable this option on the client, simply click the **Obtain DNS Server Address Automatically** option. No conflicts are caused by duplicate IP addresses.

If the **DHCP Client** service stops, your computer will not receive dynamic IP addresses and automatic dynamic DNS updates will stop being registered on the DNS server.
**DHCP Server**

The DHCP Server service allocates IP addresses and enables advanced configuration of network settings such as DNS servers and WINS servers to DHCP clients automatically. DHCP uses a client/server model. The network administrator establishes one or more DHCP servers that maintain TCP/IP configuration information and provide the information to client computers. The server database includes the following:

- Valid configuration parameters for all client computers on the network.
- Valid IP addresses that are maintained in a pool for assignment to client computers, plus reserved addresses for manual assignment.
- Duration of the lease offered by the server. The lease defines the length of time the assigned IP address is valid.

DHCP is an IP standard that is designed to reduce the complexity of address configuration administration. It uses a server computer to centrally manage IP addresses and other related configuration details for your network. The Windows Server 2003 family provides the DHCP service, which enables the server computer to perform as a DHCP server and configure DHCP-enabled client computers on your network as described in the current DHCP draft standard, Internet Engineering Task Force (IETF) Request for Comments (RFC) 2131.

DHCP includes the Multicast Address Dynamic Client Assignment Protocol (MADCAP), which is used to perform multicast address allocation. When registered client computers are dynamically assigned IP addresses through MADCAP they can participate efficiently in the data stream process, such as for real-time video or audio network transmissions.

With a DHCP server installed and configured on your network, DHCP-enabled client computers can obtain their IP addresses and related configuration parameters dynamically each time they start and join the network. DHCP servers provide this configuration in the form of an address-lease offer to the client computers.

If the DHCP Server service stops, the server will no longer issue IP addresses or other configuration parameters automatically. This service is only installed and activated if you configure a Windows Server 2003 computer as a DHCP server.

**Distributed File System**

The Distributed File System service manages logical volumes that are distributed across a local or wide area network (WAN) and is required for the Active Directory SYSVOL share. Distributed File System (DFS) is a distributed service that integrates disparate file shares into a single logical namespace.

This namespace is a logical representation of the network storage resources that are available to users on the network. If the Distributed File System service stops, you will be unable to access file shares or network data through the logical namespace. To access the data when the service is stopped, you will need to know the names of all the servers and all the shares in the namespace, and access each of these targets independently. This service is installed and run by default on Windows Server 2003 computers.
**Distributed Link Tracking Client**

The Distributed Link Tracking Client service maintains links between the NTFS file system (NTFS) files within your computer or across computers in your network domain. This service ensures that shortcuts and Object Linking and Embedding (OLE) links continue to work after the target file is renamed or moved.

When you create a shortcut to a file on an NTFS volume, distributed link tracking stamps a unique object identifier (ID) into the target file, which is known as the link source. The file that refers to the target file (known as the link client) also stores information about the object ID internally. Distributed link tracking can use this object ID to locate the link source file in the following scenarios:

- When the link source file is renamed.
- When the link source file is moved to another folder on the same volume or a different volume of the same computer.
- When the link source file is moved to another computer in the network.

**Note:** Unless the computer is in a domain where the Distributed Link Tracking Server service is available, this form of link tracking is less reliable over time.

- When the shared network folder that contains the link source file is renamed.

In a Windows 2000 or Windows Server 2003 domain in which the Distributed Link Tracking Server service is available, the link source file can be found in the following additional scenarios:

- When the computer that contains the link source file is renamed.
- When the volume that contains the link source file is moved to another computer within the same domain.

The scenarios that involve the Distributed Link Tracking Server service require that the client computer—the computer on which the Distributed Link Tracking Client service is running—have the DLT_AllowDomainMode system policy configured for clients that run Windows XP with SP1 or SP2. For all of the above scenarios, the link source file must be on an NTFS volume that runs either Windows 2000, Windows XP, or the Windows Server 2003 family. The NTFS volumes cannot be on removable media.

**Note:** The Distributed Link Tracking Client service monitors activity on NTFS volumes and stores maintenance information in a file called Tracking.log, which is located in a hidden folder called System Volume Information at the root of each volume. This folder is protected by permissions that allow only the computer to have access to it. The folder is also used by other Windows services, such as the Indexing Service.

If the Distributed Link Tracking Client service stops, any links to content on that computer will not be maintained or tracked.

**Distributed Link Tracking Server**

The Distributed Link Tracking Server service stores information so that files that are moved between volumes can be tracked for each volume in the domain. When enabled, the Distributed Link Tracking Server service runs on each domain controller in a domain. This service enables the Distributed Link Tracking Client service to track linked documents that have been moved to a location in another NTFS volume in the same domain.

The Distributed Link Tracking Server service is disabled by default. If you enable it, you must do so on all domain controllers of a domain. If the Distributed Link Tracking
Server service is enabled on a domain controller that is upgraded to a newer version of Windows Server, the service must be re-enabled manually.

If the Distributed Link Tracking Server service is enabled, then the DLT_AllowDomainMode system policy must be enabled for Windows XP client computers to be able to use it. If the Distributed Link Tracking Server service is enabled and then later disabled, purge its entries in Active Directory. For more information, see the Microsoft Knowledge Base article “Distributed Link Tracking on Windows–based domain controllers” at http://support.microsoft.com/kb/312403/.

If the Distributed Link Tracking Server service stops or if you disable it, links that are maintained by the Distributed Link Tracking Client service will eventually become less reliable.

In Windows Server 2003, the Distributed Link Tracking Server service is installed but disabled by default.

**Distributed Transaction Coordinator**

The Distributed Transaction Coordinator service coordinates transactions that are distributed across multiple computers and/or resource managers, such as databases, message queues, file systems, and other transaction–based resource managers. This service is necessary if transactional components are to be configured through COM+. It is also required for transactional queues in Message Queuing (MSMQ) and SQL Server operations that span multiple computers.

The Distributed Transaction Coordinator service is installed and active by default. If it stops, transactions that use this service will not be executed. Clustered installations of Microsoft Exchange, SQL Server, or other applications that make use of transaction services may be affected if this service stops.

**DNS Client**

The DNS Client service resolves and caches DNS names for your computer. The DNS Client service must run on every computer that performs DNS name resolution. DNS name resolution is needed to locate domain controllers in Active Directory domains. The DNS Client service is also needed to enable location of the devices that are identified through DNS name resolution.

The DNS Client service that runs on Windows Server 2003 implements the following features:

- **System-wide caching.** Resource records (RRs) from query responses are added to the client cache as applications query DNS servers. This information is then cached for a specific Time to Live (TTL) and can be used again to answer subsequent queries.

- **RFC-compliant negative caching support.** In addition to positive query responses from DNS servers (which contain resource record information in the answered reply), the DNS Client service also caches negative query responses.

A negative response results when a RR for the queried name does not exist. Negative caching prevents the repetition of additional queries for names that do not exist, which can adversely affect client computer performance. Any negative query information that is cached is kept for a shorter period of time than positive query information; by default, no more than five minutes. This configuration prevents stale negative query information from being continuously cached if the records later become available.
• **Avoidance of unresponsive DNS servers.** The **DNS Client** service uses a server search list that is ordered by preference. This list includes all preferred and alternate DNS servers that are configured for each of the active network connections on the computer. Windows Server 2003 rearranges these lists based on the following criteria:
  
  • Preferred DNS servers are given first priority.
  • If no preferred DNS servers are available, then alternate DNS servers are used.
  • Unresponsive servers are removed temporarily from these lists.

If the **DNS Client** service stops, the computer will not be able to resolve DNS names or locate Active Directory domain controllers and users may not be able to log on to the computer.

**DNS Server**

The **DNS Server** service enables DNS name resolution. It answers queries and update requests for DNS names. DNS servers are needed to locate devices that are identified by their DNS names and to locate domain controllers in Active Directory.

If the **DNS Server** service stops or if you disable it, DNS updates will not occur. The **DNS Server** service does not need to run on every computer. However, if there is no authoritative DNS server for a particular portion of the DNS namespace, then the location of the devices that use DNS names in that portion of the namespace will fail. Absence of an authoritative DNS server for the DNS namespace that is used to name Active Directory domains will result in an inability to locate domain controllers in that domain.

The **DNS Server** service is only installed and activated if you configure a Windows Server 2003 computer as a DNS server.

**Error Reporting Service**

The **Error Reporting Service** collects, stores, and reports unexpected application errors or closures to Microsoft. It also authorizes error reporting for services and applications that run in non-standard environments. This service provides Microsoft product groups with efficient and effective information to debug driver and application faults.

You can configure error reporting to send Microsoft-specific error information and to generate reports for operating system errors, Windows component errors, or program errors. An operating system error causes the computer to display a stop screen with error codes. A program or component error causes the program or component to stop working.

If you have an Internet connection, you can report these errors directly to Microsoft. You can configure error reporting to respond to program errors in one of two ways: as soon as an error occurs, the **Error Reporting** dialog box can prompt any user to send the error to Microsoft, or the next time an administrator logs on, the **Error Reporting** dialog box can prompt the administrator to send the error report to Microsoft.

Windows treats operating system errors and unplanned shutdowns differently from the way it treats program errors. When operating system errors or unplanned shutdowns occur, Windows writes the error information to a log file. The next time an administrator logs on, the **Error Reporting** dialog box prompts them to report the error. When you send an error report to Microsoft through the Internet, you provide technical information that people at Microsoft use to enhance future versions of the product. This data is used for quality control purposes only and is not used to track individual users or installations for any marketing purpose. If information is available to help you solve the problem, Windows displays an additional **Error Reporting** dialog box with a link to that information.
Alternatively, if your organization has configured Group Policy, administrators in your IT department can use Corporate Error Reporting to collect and report only those errors that they think are important. To configure workstations and servers for Corporate Error Reporting, administrators can enable the Report Errors policy setting and configure the Corporate upload file path to the local file server where the Corporate Error Reporting tool is installed. When errors occur, information is automatically redirected to this file server. Administrators can then review the error information, identify the important data, and submit it to Microsoft with the Corporate Error Reporting tool. You can download the Corporate Error Reporting tool from the Office XP Resource Kit Web site at www.microsoft.com/office/ork/xp/default.htm.

If the Error Reporting Service stops, error reporting will not occur. If the Display Error Notification setting is enabled in the Error Reporting dialog box, users will still see a message that indicates a problem occurred, but they will not have the option to report this information to Microsoft or a local network share. This service is installed and run by default.

**Event Log**

The Event Log service enables event log messages that are issued by Windows–based programs and components to be viewed in Event Viewer. These event log messages contain information that can help diagnose problems with applications, services, and the operating system. The logs can be viewed through the Event Log APIs or through the MMC Event Viewer snap-in.

By default, a computer that runs a Windows Server 2003 family operating system records events in three different logs:

- **Application log.** This log records application program events. For example, a database program might record a file error in the Application log. Program developers decide which events to log.

- **Security log.** This log records events such as valid and invalid logon attempts, as well as events that are related to resources—such as when files or other objects are created, opened, or deleted. For example, if you enable logon auditing, attempts to log on to the computer are recorded in the Security log.

- **System log.** This log records events that relate to Windows components. For example, the System log would record the failure of a driver or other component to load during startup. The event types that are logged by Windows components are predetermined by the server.

A Windows Server 2003–based computer that is configured as a domain controller records events in two additional logs:

- **Directory service log.** This log records events that relate to Active Directory. For example, connection problems between the server and the global catalog are recorded in the Directory service log.

- **File Replication service log.** This log records Windows File Replication service events. For example, file replication failures and events that occur while domain controllers are being updated with information about system volume changes are recorded in the File Replication log.

A computer that runs Windows and is configured as a DNS server records events in an additional log:

- **DNS Server log.** This log contains events that are logged by the Windows DNS service.

You cannot stop the Event Log service. If you disable the service, it would be impossible to track events, which will significantly reduce the ability to successfully diagnose
computer problems. Also, security events would not be audited, and you would not be able to view previous event logs with the MMC Event Viewer snap-in.

**Fast User Switching Compatibility**

The **Fast User Switching Compatibility** service provides management for applications that require assistance in a multiple user environment. The Fast User Switching feature in Windows XP allows multiple users who are logged on to the computer at the same time to easily switch between sessions. They do not need to shut down applications and log off.

Many programs were not designed to run in a multiple-user environment, and they can experience problems when multiple users log on to the computer. The **Fast User Switching Compatibility** service performs one of four different actions when a specific problematic program is in use and when Fast User Switching is activated:

- With Type 1 programs, the service will allow the user to close down the first instance of these programs when a second instance is launched. This action is the least intrusive, but requires the user to have administrative privileges.
- With Type 2 programs, the service closes them when the session is disconnected (either by a "Switch User" action or when the computer returns to the Welcome screen after the screen saver is dismissed).
- With Type 3 programs, the service closes them when the session is disconnected and restarts them when the user reconnects to their session. This option is good for programs that use resources that are not easily shared across multiple sessions, such as COM ports.
- With Type 4 programs, the service closes them when another user logs on. This option addresses programs that can be intrusive to the computer but do not need to be closed upon return to the Welcome screen. The program will continue to run when the user disconnects and will only be closed when another user logs on.

If you disable the **Fast User Switching Capability** service, some applications might not work properly on a computer that has the Fast User Switching feature enabled.

**Fax Service**

The **Fax Service**, a Telephony Application Programming Interface (TAPI)-compliant service, provides fax capabilities from users’ computers. The **Fax Service** allows users to send and receive faxes from their desktop applications through either a local fax device or a shared network fax device. The service offers the following features:

- Send and receive faxes
- Track and monitor fax activity
- Inbound fax routing
- Server and device configuration management
- Archiving of sent faxes

If you disable the print spooler or telephony service, the **Fax Service** will not start successfully. If this service stops, users will not be able to send or receive faxes. The **Fax Service** stops when there is no fax activity and is restarted on an as-needed basis.
**File Replication**

The **File Replication** service allows files to be automatically copied and maintained simultaneously on multiple servers. The File Replication Service (FRS) is the automatic file replication service in Windows 2000 and the Windows Server 2003 family, and its function is to replicate the contents of the system volume (SYSVOL) between all domain controllers in a domain. It can also be configured to replicate files among alternate targets that are associated with the fault-tolerant DFS.

If the **File Replication** service stops, file replication will not occur and server data will not synchronize. Also, a domain controller’s ability to function could be seriously affected if this service stops. The **File Replication** service is installed by default on Windows Server 2003, but its startup state is configured to **Manual**.

**File Server for Macintosh**

The **File Server for Macintosh** service enables Macintosh computer users to store and access files on computers that run Windows Server 2003. If you turn off this service, Macintosh client computers will not be able to store and access files on Windows Server 2003–based computers. This service is not installed or started by default.

**FTP Publishing Service**

The **FTP Publishing Service** provides FTP connectivity and administration through the Microsoft Internet Information Server (IIS) snap-in. Features include the ability to throttle bandwidth, security accounts, and extensible logging. This service includes the new FTP User Isolation feature, which allows users to access only their files on an FTP site. Also, there is improved international support.

If the **FTP Publishing Service** stops, the server cannot function as an FTP server. This service is not installed by default.

**Help and Support**

The **Help and Support** service allows the Help and Support Center application to run on users’ computers, supports the application, and enables communication between the client application and the help data. This service provides access to stores and services such as the taxonomy database that contains metadata and information about the help topics, the support automation framework that enables data collection for registered support providers, user history and preference information, and the search engine manager. When you interact with the Help and Support Center features such as search, index, or table of contents, the service allows for data transaction support of all these features.

If the **Help and Support** service is configured to **Manual**, the service will start if a user accesses the Help and Support Center from the desktop. If you disable or stop this service, the Help and Support Center application will be essentially unusable and users will see the following message:

> Windows cannot open Help and Support because a system service is not running.

Users will be able to access some high-level topics that might be cached on the local computer, but most of the Help and Support Center application features (including Remote Assistance) cannot function if the **Help and Support** service is not enabled. However, users can still view the *.HLP and *.CHM files that are located in the
Windows\Help folder. The Help and Support service is installed and started automatically by default in both Windows XP and Windows Server 2003.

**HTTP SSL**

The **HTTP SSL** service enables IIS to perform Secure Sockets Layer (SSL) functions. SSL is an open standard that establishes secure communications channels to prevent the interception of critical information, such as credit card numbers. Primarily, it enables secure electronic financial transactions on the World Wide Web, although it is designed to work on other Internet services as well.

If the **HTTP SSL** service stops, IIS will not be able to perform SSL functions. This service is installed when IIS is installed and is not present or active otherwise.

**Human Interface Device Access**

The **Human Interface Device Access** service enables generic input access to Universal Serial Bus (USB) devices such as keyboards and mice. The service activates and maintains predefined hot buttons on keyboards, remote controls, and other multimedia devices. This service is installed and started by default on Windows XP and Windows Server 2003 computers.

If the **Human Interface Device Access** service stops, hot buttons that are controlled by this service will no longer function. For instance, hotkey buttons for back, forward, volume, previous track, etc. on USB keyboards and volume buttons on USB speakers will not function.

**IAS Jet Database Access**

The **IAS Jet Database Access** service uses the Remote Authentication Dial-in User Service (RADIUS) protocol to provide authentication, authorization, and accounting services. It is only available in 64-bit versions of Windows. With Internet Authentication Services (IAS), you can centrally manage user authentication, authorization, and accounting. You can also use IAS to authenticate users against domain controllers that run Windows NT® 4.0, Windows 2000, or Windows Server 2003 operating systems. IAS works equally well in homogeneous and heterogeneous networks.

IAS can be used as a RADIUS proxy to route RADIUS messages between RADIUS clients (access servers) and RADIUS servers that perform user authentication, authorization, and accounting for the connection attempt. When used as a RADIUS proxy, IAS is a central switch or routing point through which RADIUS access and accounting messages flow. IAS records information in an accounting log about the messages that are forwarded.

A RADIUS authentication, authorization, and accounting infrastructure consists of the following components:

There are two IAS Jet databases. Ias.mdb is used to configure IAS, and Dnary.mdb is used to validate the dictionary that IAS uses to track the vendor specific attributes of RADIUS-compatible network access servers. Do not modify the Jet databases.

If the **IAS Jet Database Access** service stops, remote network access that requires user authentication will be unavailable. For example, remote access dial-up, VPN, wireless LAN (802.1x), and Ethernet 802.1x LAN access will not work. If you disable this service, both the **Routing and Remote Access Service (RRAS)** and IAS services will not start. You will also be unable to administer RRAS or IAS either locally or remotely. This service is not installed by default on any version of Windows; it is only available on the Itanium-based versions of the Windows Server 2003 family.
**IIS Admin Service**

The IIS Admin Service allows administration of IIS components such as FTP, application pools, Web sites, Web service extensions, and both Network News Transfer Protocol (NNTP) and Simple Mail Transfer Protocol (SMTP) virtual servers. If you stop or disable this service, you will not be able to run Web, FTP, NNTP, or SMTP sites.

In Windows 2000, the IIS Admin Service and related services are installed by default. In the Windows Server 2003 family, you must install the IIS components through Add/Remove Windows Components or Configure Your Server.

**IMAPI CD-Burning COM Service**

The IMAPI CD-Burning COM Service manages the creation of CDs through the Image Mastering Applications Programming Interface (IMAPI) COM interface and performs CD-Recordable (CD-R) writes when requested by the user through Windows Explorer, Windows Media® Player (WMP) or third-party applications that use this API. IMAPI allows an application to stage and burn simple audio or data images to CD-R and CD Rewritable (CD-RW) devices. The API supports Redbook audio and data disc formats with both Joliet and ISO 9660. The architecture allows for future expansion of the supported format set.

If the IMAPI CD-Burning COM Service stops or if you disable it, your computer will be unable to record CDs with the built-in features of Windows XP and Windows Server 2003. If you turn off this service and use a third party CD-RW application, your ability to record CDs will not be affected (if the third-party software does not rely on the service). If this service is started after logon, you must log off of your computer and then log back on to write data to CD-R media with your CD-R device through Windows Explorer. This service is installed by default on Windows XP, but it is not started until a user requests CD-R writing through Windows Explorer. It is installed but disabled by default on Windows Server 2003.

**Indexing Service**

The Indexing Service indexes the contents and properties of files on local and remote computers and provides rapid access to files through a flexible querying language. The Indexing Service also enables quick document search capability on local and remote computers and a search index for content that is shared on the Web. The service builds indexes of all textual information in files and documents. After the initial index build is complete, the Indexing Service maintains its indexes whenever a file is created, modified, or deleted.

Initial indexing can be resource-intensive. By default, the Indexing Service is set to start manually. When the service is active it will index only when the computer is idle, although you can use the MMC Index snap-in to configure the service to work at non-idle times. MMC also allows you to optimize the service’s resource allocation configuration for query or indexing usage patterns.

If the Indexing Service stops, text-based searches will be slower.

**Infrared Monitor**

The Infrared Monitor service enables you to share files and images through infrared connections. This service is installed by default on Windows XP if an infrared device is detected during operating system installation. This service is not available on Windows Server 2003 Web, Enterprise, or Datacenter Server editions.
If the Infrared Monitor service stops, files and images cannot be shared through infrared connections.

**Internet Authentication Service**

The Internet Authentication Service (IAS) performs centralized authentication, authorization, audit, and accounting of users who connect to a network—either LAN or remote—through VPN equipment, Remote Access Equipment (RAS), or 802.1x Wireless and Ethernet/Switch Access Points.

IAS implements the IETF standard RADIUS protocol, which enables heterogeneous network access equipment. If IAS stops or if you disable it, authentication requests will fail over to a backup IAS server, if it is available. If no backup IAS servers are available, users will not be able to connect to the network. This service must be installed manually and is only available on members of the Windows Server 2003 family.

**Intersite Messaging**

The Intersite Messaging service enables message exchanges between computers that run Windows Server sites. This service is used for mail-based replication between sites. Active Directory includes support for replication between sites through SMTP over IP transport. SMTP support is provided by the SMTP service, which is a component of IIS.

The set of transports that are used for communication between sites must be extensible. Therefore, each transport is defined in a separate add-in dynamic link library (DLL) file. These add-in DLL files are loaded into the Intersite Messaging service, which runs on all domain controllers that can perform communication between sites. The Intersite Messaging service directs send and receive requests to the appropriate transport add-in DLL files, which then route the messages to the Intersite Messaging service on the destination computer.

If the Intersite Messaging service stops, messages will not be exchanged, intersite messaging replication will not work, and site-routing information will not be calculated for other services. This service is installed by default on Windows Server 2003 computers, but it is disabled until the server is promoted to the domain controller role.

**IP Version 6 Helper Service**

The IP Version 6 Helper Service offers Internet Protocol version 6 (IPv6) connectivity over an Internet Protocol version 4 (IPv4) network. IPv6 is a new suite of standard protocols for the network layer of the Internet. It is designed to solve many IPv4 problems with regard to address depletion, security, auto-configuration, and extensibility. This service, often referred to as "6to4," allows IPv6-enabled sites and hosts to communicate through IPv6 over an IPv4 infrastructure—for example, the Internet. IPv6 sites and hosts can use their 6to4 address prefix and the Internet to communicate. They do not need to obtain an IPv6 global address prefix from an Internet service provider (ISP) and connect to the 6bone—the IPv6-enabled portion of the Internet.

6to4 is a tunneling technique that is described in RFC 3056. 6to4 hosts do not require any manual configuration and uses standard auto-configuration to create 6to4 addresses. 6to4 uses the global address prefix of 2002:WWXX:YYZZ::/48, where WWXX:YYZZ is the colon-hexadecimal representation of a public IPv4 address (w.x.y.z) that is assigned to a site or host, also known as the Next Level Aggregator (NLA) portion of a 6to4 address.

The IPv6 Helper Service also supports 6over4, also known as IPv4 multicast tunneling, a technique that is described in RFC 2529. 6over4 allows IPv6 and IPv4 nodes to
communicate through IPv6 over an IPv4 infrastructure. 6over4 uses the IPv4 infrastructure as a multicast-capable link. For 6over4 to work correctly, the IPv4 infrastructure must be IPv4 multicast-enabled.

If the IP Version 6 Helper Service stops, the computer will only have IPv6 connectivity if it is connected to a native IPv6 network. This service is not installed or activated by default.

**IPSec Policy Agent (IPSec Service)**

The **IPSec Policy Agent (IPSec Service)** service provides end-to-end security between clients and servers on TCP/IP networks, manages IPSec policy, starts the Internet Key Exchange (IKE) and coordinates IPSec policy settings with the IP security driver. The service is controlled by using the NET START or NET STOP command.

IPsec operates at the IP layer and is transparent to other operating system services and applications. The service provides packet filtering, and can negotiate security between computers on IP networks. You can configure IPsec to provide:

- Packet filtering with actions to permit, block, or negotiate security.
- Negotiated trust and secure IP communication. The IKE protocol mutually authenticates the sender and receiver of IP data packets based on policy settings. Authentication can use the Kerberos authentication protocol, digital certificates, or a shared secret key (password). IKE automatically generates cryptographic keys and IPSec security associations.
- Protect IP packets with IPSec secure formats that provide cryptographic integrity, authenticity, and (optionally) encryption of IP packets.
- Secure end-to-end connections through IPSec transport mode.
- Secure IP tunnels through IPSec tunnel mode.

IPsec also provides security for Layer Two Tunneling Protocol (L2TP) VPN connections. If the **IPSec Policy Agent (IPSec Service)** service stops, it will impair TCP/IP security between clients and servers on the network. This service is installed and activated by default on Windows Server 2003 and Windows XP computers.

**Kerberos Key Distribution Center**

The **Kerberos Key Distribution Center** service enables users to log on to the network and be authenticated by the Kerberos v5 authentication protocol.

As in other implementations of the Kerberos protocol, the Kerberos Key Distribution (KDC) is a single process that provides two services:

- **Authentication Service.** This service issues ticket-granting tickets (TGTs) for connection to the ticket-granting service in its own domain or in any trusted domain. Before a client computer can request a ticket to another computer, it must request a TGT from the authentication service in its account domain. The authentication service returns a TGT for the ticket-granting service in the target computer’s domain. The TGT can be reused until it expires, but first access to any domain's ticket-granting service always requires the client computer to contact the authentication service in its account domain.

- **Ticket-Granting Service (TGS).** This service issues tickets for connection to computers in its own domain. When a client computer wants to access another computer, it must request a TGT and ask for a ticket to the computer. The ticket can be reused until it expires, but first access to any computer always requires contact with the ticket-granting service in the target computer’s account domain.
If the Kerberos Key Distribution Center service stops, users will be unable to log on to the network and access resources. This service is installed on all Windows Server 2003 computers, but it only runs on domain controllers. If you disable this service, users will not be able to log on to the domain.

**License Logging Service**

The License Logging Service monitors and records client access license information. It works with portions of the operating system, such as IIS, Terminal Services, file and print sharing, and also with products that are not a part of the operating system, such as SQL Server or Microsoft Exchange server.

If the License Logging Service stops or if you disable it, licensing will be enforced but will not be monitored. This service is disabled by default on Windows Server 2003 computers.

**Logical Disk Manager**

The Logical Disk Manager service detects and monitors new hard disk drives and sends disk volume information to the Logical Disk Manager Administrative Service for configuration. This service monitors Plug and Play events to detect new drives and uses an administrator service and a watchdog service. Do not disable the service if dynamic disks are present in the computer.

The Logical Disk Manager service runs by default on Windows Server 2003 and Windows XP computers. If it stops, dynamic disk status and configuration information might become outdated. For example, hard disk drives will not be detected. The administrator service and the watchdog service are essentially one component. The administrative service only starts when you configure a drive, partition, or when a new drive is detected.

**Logical Disk Manager Administrative Service**

The Logical Disk Manager Administrative Service performs administrative services for disk management requests and configures hard disk drives and volumes. It only starts when you configure a drive or partition, or when a new drive is detected. This service does not start by default, but is activated whenever dynamic disk configuration changes occur or when the MMC Disk Management snap-in or the Diskpart.exe tool are opened. Changes that can activate this service include conversions of basic disks to dynamic, recovery of fault-tolerant volumes, volume formatting, or changes to a page file.

The Logical Disk Manager Administrative Service only runs for configuration processes and then stops. If you disable this service, attempts to use the MMC Disk Management snap-in to configure disks will display the following error message:

Unable to connect to Logical Disk Manager service

**Machine Debug Manager**

The Machine Debug Manager service manages local and remote debugging for a number of applications, including the Microsoft Script Editor, various versions of the Office application suite, and Microsoft Visual Studio.
If you disable the **Machine Debug Manager** service, attempts to debug scripts or processes will fail and display the following error message:

Unable to start debugging. The Machine Debug Manager Service is disabled.

Also, users will not be given the opportunity to debug script errors in Web pages.

**Message Queuing**

The **Message Queuing** service is a messaging infrastructure and development tool that can be used to create distributed messaging applications for Windows. Such applications can communicate across heterogeneous networks and send messages between computers that may be temporarily unable to connect to each other. This service provides guaranteed message delivery, efficient routing, security, and priority-based messaging. It also supports the ability to send messages within transactions, and it provides both Microsoft Win32® and COM APIs for all programmatic functionality, including administration and management.

The implementation of the remote read features in the Windows XP version of the **Message Queuing** service allows unauthenticated users to connect to queues. A malicious user could purge a queue and create a denial of service condition. Also, Message Queuing remote read data is transmitted over the network in plaintext, which means it could be read by a malicious user who is able to capture network data.

For these reasons, Microsoft recommends that you not install the **Message Queuing** service on Windows XP computers that are exposed to untrusted networks such as the Internet. The service is not installed by default in Windows XP, so most organizations should be protected from this vulnerability already.

If the **Message Queuing** service stops, distributed messages will be unavailable. If you disable this service, any services that explicitly depend on it will not start. Also, **COM+ Queued Component (QC)** functionality, some functionality of Windows Management Instrumentation (WMI), and the **Message Queuing Triggers** service will be affected. This service is not installed by default on Windows Server 2003 computers.

**Message Queuing Down Level Clients**

The **Message Queuing Down Level Clients** service provides Active Directory access for Windows NT 4.0, Windows 9x, and Windows 2000 clients that use the **Message Queuing** service on domain controllers. The **Message Queuing** service optionally uses information that is published in Active Directory to obtain routing information for security-related objects, such as destination public keys, and to learn about public queues. If you install **Message Queuing** in workgroup mode, then Active Directory is never accessed. This service is only required on Windows Server 2003 domain controllers that run the **Message Queuing** service.

If the **Message Queuing Down Level Clients** service stops on a domain controller, then versions of the Microsoft Message Queuing client earlier than version 3.0 will not be able to obtain Active Directory services on the specified domain controller for public queue discoverability, message routing, and site recognition. This service is not installed by default on Windows Server 2003 computers.
### Message Queuing Triggers

The **Message Queuing Triggers** service provides a rule-based system to monitor messages that arrive in a **Message Queuing** service queue and, when the conditions of a rule are satisfied, invoke a COM component or a stand-alone executable program to process the message.

The **Message Queuing Triggers** service is installed as an integral part of the **Message Queuing** service, which is an optional Windows component that is available on all versions of Windows except Windows XP Home Edition.

If the **Message Queuing Triggers** service stops, you will not be able to apply rule-based monitoring or invoke programs to process messages automatically. This service is not installed by default on Windows Server 2003 computers.

### Messenger

The **Messenger** service sends messages to or receives messages from users, computers, administrators, and the **Alerter** service. This service is not related to Windows Messenger, a free instant-messaging service that is available through MSN.

If you disable the **Messenger** service, notifications cannot be sent to or received by the computer or by users who are currently logged on. Also, the NET SEND and NET NAME shell commands will no longer function. This service is installed but disabled by default on Windows Server 2003 and Windows XP computers.

### Microsoft POP3 Service

The **Microsoft POP3 Service** provides e-mail transfer and retrieval services. Administrators can use this service to store and manage e-mail accounts on a mail server. When you install the **Microsoft POP3 Service** on a mail server, users can connect to that server and retrieve e-mail messages with an e-mail client program that supports the POP3 protocol, such as Microsoft Outlook®. The **Microsoft POP3 Service** works in combination with the **SMTP Service**, which allows users to send outgoing e-mail.

The **Microsoft POP3 Service** is the mechanism that allows users to retrieve their e-mail messages from a mail server. Sender's and recipient's computers connect to the Internet through their respective Internet service providers (ISPs). When the sender uses an e-mail client to send a message, the **SMTP Service** transfers the message to the sender's ISP. The message is then routed to the Internet and relayed through various intermediate servers. When the message reaches the recipient's ISP, it is placed in the recipient's mailbox. When the recipient's computer connects to their ISP, the ISP transfers the message to the recipient's e-mail client on the local computer in accordance with POP3 protocol standards.

If the **Microsoft POP3 Service** stops, e-mail transfer and retrieval services will no longer function. This service must be manually installed on Windows Server 2003 computers.

### Microsoft Software Shadow Copy Provider

The **Microsoft Software Shadow Copy Provider** service manages software-based shadow copies that are taken by the **Volume Shadow Copy** service. A shadow copy is a snapshot copy of a disk volume that represents a consistent read-only point in time for that volume. This point-in-time snapshot then stays constant and allows an application, such as backup software, to copy data from the shadow copy to tape.
There are two general classes of shadow copies:

- **Hardware.** A hardware shadow copy is a mirror of two or more disks that are split into separate volumes. One of the two volumes remains the working set and the other one can be mounted separately.

- **Software.** A software shadow copy uses a copy-on-write scheme to copy all sectors of a volume that change over time into a differential area on disk. When the shadow copy is mounted, all unchanged sectors are read from the original volume and all sectors that have changed are read from the differential area.

Shadow copies can resolve three classic data backup challenges:

- The need to back up files that were opened for exclusive access. Backup of an open file is a challenge, because it is likely in a state of change. Without a shadow copy or a way to suspend the application, backups often become corrupted.

- The need to maintain a computer's availability during the shadow copy.

- Use of the same communications channels as snapshots to facilitate information transfer between application and backup tools.

The platform for shadow copies consists of the following:

- A set of shadow copy APIs, which handle application synchronization. This synchronization ensures that a shadow copy is good because application data is in a state that is known to be valid. These APIs provide the required functionality for plug-in shadow copy providers and multi-volume shadow copy coordination.

- A shadow copy device driver that copies old sectors to a "difference file" when they are first replaced to provide volume shadow copies for any locally mounted volume. The "difference file" is laid over the current volume to synthesize the shadow copy volume.

- Support in the software development communities for the sync and provider APIs.

If the **Microsoft Software Shadow Copy Provider** service stops, software-based volume shadow copies cannot be managed, which could cause Windows Backup to fail. This service is installed by default on Windows Server 2003, but it only runs when requested.

**MSSQL$UDDI**

The **MSSQL$UDDI** service is installed when the Universal Description, Discovery, and Integration (UDDI) feature of the Windows Server 2003 family is installed. (This feature provides UDDI capabilities within an organization.) When this service is installed, a SQL Server database instance is also installed. This instance manages all of the files that comprise the databases that are used by the service, and it processes all Transact-SQL statements that are sent from SQL Server client applications. The **MSSQL$UDDI** service allocates computer resources effectively between multiple concurrent users. It also enforces business rules that are defined in stored procedures and triggers, ensures the consistency of the data, and prevents logical problems, such as two people who try to update the same data at the same time.

UDDI is an industry specification for the description and discovery of Web services. The UDDI specification builds on the Simple Object Access Protocol (SOAP), Extensible Markup Language (XML), and HTTP/S protocol standards that were developed by the World Wide Web Consortium (W3C) and the IETF. UDDI services are standards-based XML Web services that allow developers to efficiently publish, discover, share, and re-use Web Services directly through their development tools. Built on the Microsoft .NET Framework, UDDI services use proven Microsoft SQL Server technology and tools to provide a scalable storage mechanism. IT managers can leverage UDDI services’
support for standard categorization schemes and Active Directory authentication, which allows easy integration within an enterprise environment.

The MSSQL$UDDI service must be manually installed on Windows Server 2003 computers; when installed, its startup type is configured to Manual. If this service stops, the UDDI SQL Server database will no longer be available and clients will no longer be able to query or access the data in its databases.

**MSSQLServerADHelper**

The MSSQLServerADHelper service enables Microsoft SQL Server and Microsoft SQL Server Analysis Services to publish information in Active Directory when those services are not invoked by the Local System account. Only one instance of MSSQLServerADHelper service is allowed to run on a computer. All instances of Microsoft SQL Server and Microsoft SQL Server Analysis Services use it on an as-needed basis.

MSSQLServerADHelper is not a server service and does not service requests from the client. The service does not use a UDP or TCP port.

You cannot stop the MSSQLServerADHelper service. This service is dynamically started by an instance of SQL Server or Analysis Manager when needed. The service stops as soon as it has completed its work. This service should always be run by the Local System account; do not start it manually from the console. If you disable this service, the ability to add, update, or delete SQL Server-related Active Directory objects may be affected. This service must be manually installed on Windows Server 2003 computers. When installed, its startup type is configured to Manual.

**.NET Framework Support Service**

The .NET Framework Support Service notifies a subscriber client when a specified process initializes the Client Runtime Service. The .NET Framework Support Service provides a run-time environment called the Common Language Runtime (CLR), which manages code execution and provides services that make the development process easier. Compilers and tools expose the runtime’s functionality and enable you to write code that benefits from this managed execution environment. The CLR enables you to design components and applications whose objects interact across languages. Objects that are written in different languages can communicate with each other, and their behaviors can be tightly integrated. This service is normally installed as part of the Visual Studio.NET development environment and will not be present or active unless manually installed.

If the .NET Framework Support Service stops or if you disable it, the user will not receive a notification when a .NET application starts the CLR.

**Net Logon**

The Net Logon service maintains a secure channel between your computer and the domain controller that it uses to authenticate users and services. It passes user credentials through the secure channel to a domain controller and returns the domain security identifiers and user rights for the user, which is commonly referred to as pass-through authentication. The service is installed on all Windows Server 2003 and Windows XP computers, and its startup type is set to Manual. After the computer joins a domain, the service starts automatically.

In the Windows 2000 Server family and the Windows Server 2003 family, the Net Logon service publishes service resource records in DNS and uses DNS to resolve names to
the IP addresses of domain controllers. The service also implements the replication
protocol that is based on remote procedure call (RPC) to synchronize Windows NT 4.0
primary domain controllers (PDCs) and backup domain controllers (BDCs).

If the **Net Logon** service stops, the computer may not authenticate users and services
and the domain controller cannot register DNS records. Specifically, it might deny NTLM
authentication requests, and domain controllers will not be discoverable by client
computers.

**NetMeeting Remote Desktop Sharing**

The **NetMeeting Remote Desktop Sharing** service allows authorized users to remotely
access your Windows desktop with the Microsoft NetMeeting® application from another
personal computer over an intranet. The service is installed and disabled by default. It
must be explicitly enabled by the user through NetMeeting, and can be disabled in
NetMeeting or shut down by means of a Windows tray icon.

If the **NetMeeting Remote Desktop Sharing** service stops or if you disable it, the
NetMeeting display driver is unloaded and the computer will not be able to provide
remote access to its desktop.

**Network Connections**

The **Network Connections** service is installed by default on Windows Server 2003 and
Windows XP computers. This service manages objects in the **Network Connections**
folder, from which you can view both network and remote connections. This service is
responsible for client network configuration and displays connection status in the
notification area on the taskbar. You may also view and configure network interface
settings through this service.

The **Network Connections** service will start automatically when the startup type is
Manual and the Network Connections interface is invoked. If this service stops, client-
side configuration of LAN, dial-up, and VPN connections will be unavailable. If you
disable this service, the following might result:

- Connections will not display in the **Network Connections** folder, which will prevent
dial-out access and configuration of LAN settings.
- Other services that use Network Connections to check for Network Location-aware
  Group Policies will not function properly.
- Events that pertain to media connects and disconnects will not be received.
- Internet connection sharing will not function correctly.
- The ability to configure incoming connections, wireless settings, or your home
  network will be unavailable.
- New connections will not be created.
- Any services that explicitly depend on this service will not start.

**Network DDE**

The **Network DDE** service provides network transport and security for Dynamic Data
Exchange (DDE) for programs that run on the same computer or on different computers.
You can create Network DDE "shares" programmatically or with Ddeshare.exe and make
them visible to other applications and computers. Traditionally, the user who creates the
share will create and run a server process to handle inbound requests from client
processes and/or applications, whether they run on the same computer or remotely. After
they are connected, these processes can exchange any kind of data over a secure network transport.

This service is installed but disabled by default. To use network DDE functionality, you must set the service startup type to Manual, after which the service is only started when invoked by an application that uses Network DDE, such as Clipbrd.exe or Ddeshare.exe.

If the Network DDE service stops, DDE transport and security will be unavailable. If you disable this service, any applications that depend on it will time out when they try to start the service. If an application on a remote computer tries to start the Network DDE service on another computer, the remote computer will not be visible on the network.

**Network DDE DSDM**

The Network DDE DSDM service manages DDE network shares. This service is used only by the Network DDE service to manage shared DDE conversations. You can create and trust DDE shares with Ddeshare.exe to allow remote computers and applications to connect and share data. The Network DDE DSDM service maintains a database of DDE shares that includes information about trusted shares. For each connection request that is made from or to an application, the service queries the database and validates your security settings to determine if the request should be granted.

The Network DDE DSDM service is installed but disabled by default. To use network DDE functionality, you must set the service startup type to Manual, after which the service is only started when invoked by an application that uses Network DDE. If the Network DDE DSDM service stops, DDE network shares will be unavailable. If you disable this service, any applications that depend on it will time out when they try to start the service.

**Network Location Awareness (NLA)**

The Network Location Awareness (NLA) service collects and stores network configuration information, such as IP address and domain name changes, as well as location change information. The service notifies compatible applications when this information changes so that they can reconfigure themselves to use the current network connection.

The Network Location Awareness (NLA) service is a default service on Windows XP. Even if you configure this service with a startup type of Manual, it will usually be started by dependent services. If this service stops, network location awareness functionality will not be available.

**Network Provisioning Service**

The Network Provisioning Service provides the ability to download and manage XML configuration files from network provisioning services such as the Microsoft Wireless Provisioning Services (WPS), which enable automatic network provisioning for Internet service providers and private networks. This service works with the Wireless Zero Configuration service to provide support for the latest wireless security standards.

If the Network Provisioning Service stops or if you disable it, wireless network interface configuration and operation may not succeed, even if the network environment does not use WPS or an equivalent.
**Network News Transfer Protocol (NNTP)**

The **Network News Transfer Protocol (NNTP)** service allows computers that run Windows Server 2003 to act as news servers. Client computers can use a news client application such as the Microsoft Outlook Express messaging client to retrieve newsgroups from the server and read headers or bodies of the articles in each newsgroup. The client computers can then post back to the server.

NNTP is an Internet standard. The NNTP service that is included with Windows Server 2003 does not support feeds, in which two news servers replicate their contents between each other. However, the version that is included with Exchange 2000 does include this functionality. This service is not installed or enabled by default. It can only be installed in conjunction with IIS.

If the **Network News Transfer Protocol (NNTP)** service stops, client computers will not be able to connect and read or retrieve posts.

**NTLM Security Support Provider**

The **NTLM Security Support Provider** service provides security to RPC programs that use transports other than named pipes. It also enables users to log on to the network and be authenticated by the NTLM authentication protocol, which authenticates clients that do not use the Kerberos version 5 authentication protocol.

The Windows NT Challenge/Response NTLM authentication protocol is used on networks that include systems that run versions of the Windows NT operating system and on stand-alone systems. NTLM stands for Windows NT LAN Manager, a name that was chosen to distinguish this more advanced challenge/response-based protocol from its weaker predecessor LAN Manager (LM).

Windows 2000 used the Kerberos version 5 authentication protocol, which provides greater security to computer networks than NTLM. Although the Kerberos protocol is the authentication protocol of choice for Windows 2000 and Windows Server 2003 networks, NTLM is still supported and must be used for network authentication if the network includes computers that run versions of Windows NT, Windows 98, or Windows Millennium Edition. Logon authentication on stand-alone computers also requires NTLM.

NTLM credentials are based on data that is obtained during the interactive logon process and consist of a domain name, a user name, and a one-way hash of the user's password. NTLM uses an encrypted challenge/response protocol to authenticate a user, but does not send the user's password over the network. Instead, the computer that requests authentication must perform a calculation that proves it has access to the secured NTLM credentials.

Interactive NTLM authentication over a network typically involves two computers: a client computer, in which the user is requesting authentication, and a domain controller that stores information that is related to the user's password. Non-interactive authentication—which may be required to permit an already logged-on user to access a resource such as a server application—typically involves three computers: a client, a server, and a domain controller that does the authentication calculations on behalf of the server.

The **NTLM Security Support Provider** service is installed and runs by default on all Windows XP and Windows Server 2003 computers. If this service stops or if you disable it, clients that use the NTLM authentication protocol will not be able to log on or access network resources. Microsoft Operations Manager (MOM) relies on this service.
Performance Logs and Alerts

The Performance Logs and Alerts service collects performance data from local or remote computers based on preconfigured schedule parameters, then writes the data to a log or triggers an alert. This service starts and stops each named performance data collection based on the information that is contained in the named log collection setting. This service only runs if at least one collection is scheduled. However, it is installed by default on Windows XP and Windows Server 2003.

If the Performance Logs and Alerts service stops or if you disable it, performance information will not be collected. Also, any data collections that are currently active will terminate and future scheduled collections will not occur.

Plug and Play

The Plug and Play service enables a computer to recognize and adapt to hardware changes with little or no user input. This service enables you to add or remove devices without any detailed knowledge of your computer hardware, and you do not need to manually configure the hardware or the operating system. For example, you can plug in a USB keyboard and the Plug and Play service will detect the new device, find a driver for it, and install it. Or you can dock a portable computer and use the docking station’s Ethernet card to connect to the network; you do not need to change any configuration settings. Then you can undock the same computer and use a modem to connect to the network—again, without any manual configuration changes.

The Plug and Play service is installed and configured to run automatically on Windows Server 2003 and Windows XP. You cannot stop or disable the service through the MCC Services snap-in because of the impact on operating system stability. If you use the MSCONFIG troubleshooting tool and this service stops, the Device Manager interface will appear blank and no hardware devices will be displayed.

Portable Media Serial Number

The Portable Media Serial Number service retrieves the serial number of any portable music player that is connected to your computer. The service allows Windows Media Device Manager (WMDM) to acquire the serial number from portable music devices so that media content can be copied securely to those devices. Without the serial number, you cannot associate content to a specific device, which might prevent protected content from being transferred to the device.

To uniquely identify portable media, many storage media manufacturers have implemented a unique serial number that is stored on a non-volatile area of the storage device. For example, the CompactFlash Association (CFA) CompactFlash specification revision 1.3 requires CompactFlash cards to have a unique serial number. Some types of removable storage media also have unique serial numbers on them.

For a portable media reader or adapter to be Windows Media-compliant, it must allow an application to retrieve media serial numbers.

The Portable Media Serial Number service is installed by default on Windows XP and Windows Server 2003. Its startup type is configured to Manual, and it is launched on request by WMDM. If the service stops or if you disable it, protected content might not be allowed to transfer to the device and the serial number might not be retrieved from portable media devices.
**Print Server for Macintosh**

The Print Server for Macintosh service enables Apple Macintosh clients to route print jobs to a print spooler that is located on a computer that runs Windows Server 2003. This service also allows Windows Server 2003 Enterprise Edition to communicate with a print device that uses the AppleTalk protocol. This service is not installed by default.

If the Print Server for Macintosh service stops, Macintosh AppleTalk clients will not be able to route print jobs to a Windows Server 2003–based print spooler.

**Print Spooler**

The Print Spooler service manages all local and network print queues and controls all print jobs. The print spooler communicates with printer drivers and input/output (I/O) components, such as the USB port and the TCP/IP protocol suite, and is the center of the Windows printing subsystem. It is installed and activated by default on Windows XP and Windows Server 2003 computers.

If the Print Spooler service stops, you will not be able to either print or send faxes from your local computer. When the Print Spooler service stops on a server that runs Terminal Services, the System hive of the registry will slowly grow until it fills the system volume and causes the server to crash. This problem is caused by the fact that when new clients log on to the server through Terminal Services, the system automatically tries to map the client's local printer to a printer port on the server, and it records this mapping in the registry. However, the Print Spooler service is supposed to delete each record when the user ends their session, and if the service is not running the unused records will never be deleted.

Also, the Printer Pruner feature of Active Directory relies on the Print Spooler service. For the Printer Pruner to operate across the organization and allow orphaned queues to be scavenged on an unmanaged basis, every site in the organization must have at least one domain controller that runs the Print Spooler service. If you configure this service to Disabled or Manual, it will not automatically start when print jobs are submitted.

**Protected Storage**

The Protected Storage service protects storage of sensitive information, such as private keys, and prevents access by unauthorized services, processes, or users. The service provides a set of software libraries that allow applications to retrieve security and other information from personal storage locations as it hides the implementation and details of the storage itself.

The storage location that is provided by this service is secure and protected from modification. The Protected Storage service uses the Hash-Based Message Authentication Code (HMAC) and the Secure Hash Algorithm 1 (SHA1) cryptographic hash function to encrypt the user's master key. This component requires no configuration.

The Protected Storage service was originally introduced in Windows 2000. In Windows XP and Windows Server 2003, this service was replaced by the Data Protection API (DPAPI), which is currently the preferred service for protected storage. Unlike DPAPI, the interface to the Protected Storage service is not publicly exposed.

If the Protected Storage service stops, private keys will be inaccessible, the Windows Certificate Services service will not operate, Secure Multipurpose Internet Mail Extensions (S/MIME) and SSL will not work, and smart card logon will fail.
**QoS RSVP Service**

Quality of Service (QoS) is an industry-wide standard that was developed to achieve more efficient use of network resources. It allows clients and servers to differentiate between different data types and to prioritize end-to-end network traffic. The IETF (Internet Engineering Task Force) has played a central role to help ensure that QoS standards enable all affected network devices to participate in the end-to-end QoS-enabled connection. Quality of Service provides applications (or network administrators) with a means by which network resources—such as available bandwidth and latency—can be predicted and managed on both local computers and devices throughout the network.

The QoS RSVP Service implements Windows’ QoS support. It is installed by default on Windows XP, but is not installed on Windows Server 2003 computers. When installed, its startup type is configured to Manual. If this service is disabled or uninstalled, the computer will not be able to participate in QoS connections or make resource reservation requests for QoS-controlled bandwidth.

**Remote Access Auto Connection Manager**

The Remote Access Auto Connection Manager service detects unsuccessful attempts to connect to a remote network or computer and provides alternate methods for connection. When a program fails in an attempt to reference a remote DNS or NetBIOS name or address or when network access is unavailable, the service displays a dialog box that allows you to make a dial-up or VPN connection to the remote computer.

To assist you, the Remote Access Auto Connection Manager service maintains a local database of connections that were previously used to reach named computers or shares. When the service detects an unsuccessful attempt to reach a remote computer or share, it will offer to dial the connection that was last used to reach this remote device. This service is installed by default on Windows XP and Windows Server 2003 computers, but its startup type is configured to Manual. It is started automatically on an as-needed basis. If you disable the Remote Access Auto Connection Manager service, you will need to manually establish connections to remote computers when you need to access them.

**Remote Access Connection Manager**

The Remote Access Connection Manager system service manages dial-up and VPN connections from your computer to the Internet or other remote networks. When you double-click a connection in the Network Connections folder and click the Connect button, the Remote Access Connection Manager service either dials the connection or sends a VPN connection request and handles subsequent negotiations with the remote access server to set up the connection.

The Remote Access Connection Manager service will unload itself when no requests are pending. The Network Connections folder calls this service to enumerate the set of connections and to display the status of each one. Although its default startup state is configured to Manual, this service will be started if there are one or more VPN or dial-up connections in the Network Connections folder.

If the Remote Access Connection Manager service stops or if you disable it, your computer will not be able to make dial-up or VPN connections to a remote network or accept inbound connection requests. Also, the Network Connections folder will not display any VPN or dial-up connections, and the Internet Options Control Panel will not allow the user to configure any options that pertain to dial-up or VPN connections.
Remote Administration Service

The Remote Administration Service performs the following remote administration tasks when a server restarts:

- Increments the server boot count.
- Generates a self-signed certificate.
- Raises an alert if the date and time has not been set on the server.
- Raises an alert if the Alert E-mail functionality has not been configured.

The Remote Administration Service starts to execute the appropriate tasks when it is requested to do so by the Remote Server Manager through a COM interface. The service uses the Local System account, and requests on the COM interface are only accepted from clients that use the Administrator or Local System accounts.

If the Remote Administration Service is configured to Manual, it will start when called by the Remote Server Manager service. It can subsequently be stopped with no effect on any server functionality. This service installs and is configured to automatically start by default on Windows Server 2003 computers.

If the Remote Administration Service stops, some Remote Administration Tools features may not function properly, such as Web interface for remote administration.

Remote Desktop Help Session Manager

The Remote Desktop Help Session Manager service manages and controls the Remote Assistance feature within the Help and Support Center application (Helpctr.exe). It is installed by default on Windows XP and Windows Server 2003, but it is only started when a Remote Assistance request is made or received.

If the Remote Desktop Help Session Manager service stops, Remote Assistance and the ability to request help through Remote Assistance will be unavailable.

Remote Installation

The Remote Installation service provides the ability to install Windows 2000, Windows XP, and Windows Server 2003 on Pre-Boot Execution Environment (PXE) remote boot-enabled client computers. The Boot Information Negotiation Layer (BINL) service, the primary component of Remote Installation Services (RIS), answers PXE clients, checks Active Directory for client validation, and passes client information to and from the server. The BINL service is installed when you add the RIS component from Add/Remove Windows Components or when you select it during initial operating system installation.

RIS is a Windows deployment feature that is included in the Windows Server 2003 family. With RIS, you can support on-demand image-based or script-based operating system installations over a network connection from a RIS server to a client computer. RIS is designed to simplify the deployment of operating systems and applications and to improve failure recoverability.

You can use RIS in a variety of ways, including the following:

- Provide an operating system to users on demand. You can use RIS to create automated installation images of Windows Server 2003 family operating systems, Windows XP, and Windows 2000. When a user starts a client computer, even if that computer contains no operating system, the RIS server can respond by installing an operating system over the network; no CD is required. To support this capability, client computers must use PXE through the network adapter.
• Provide operating system images that include specific settings and applications, such as an image that complies with an organization’s desktop standard. A particular group of users can be offered the image or images that you designate for that group.

The Remote Installation service is not installed by default. If you install the service and then stop it, PXE-enabled client computers will be unable to install Windows remotely or use other RIS-based tools from the computer.

**Remote Procedure Call (RPC)**

The Microsoft Remote Procedure Call (RPC) service is a secure inter-process communication (IPC) mechanism that enables data exchange and invocation of functionality that resides in a different process. The different process can be on the same computer, on the local area network, or across the Internet. The Remote Procedure Call (RPC) service serves as the RPC endpoint mapper and COM Service Control Manager (SCM). More than 50 services depend on the RPC service to start successfully.

You cannot stop or disable the Remote Procedure Call (RPC) service. If this service is not available, the operating system will not load.

**Remote Procedure Call (RPC) Locator**

The Remote Procedure Call (RPC) Locator service enables RPC clients that use the RpcNs* family of APIs to locate RPC servers. It also manages the RPC name service database. This service is turned off by default, and it has not been used by many applications that were published after Windows 95 shipped.

For more information about the RpcNs family of APIs, see the SDK information in the MSDN Library link on the Web Resources page at www.microsoft.com/windows/reskits/webresources.

If the Remote Procedure Call (RPC) Locator service stops or if you disable it, RPC clients that need to locate RPC services on other computers may be unable to locate servers, or they may fail to start. RPC clients that rely on RpcNs* APIs from the same computer might not be able to find RPC servers that support a given interface. If the service stops or if you disable it on a domain controller, RPC clients that use the RpcNs* APIs and the domain controller might experience interruption of service when they try to locate clients. RpcNs* APIs are not used internally in Windows; you only need to start this service if third-party applications require this service.

**Remote Registry Service**

The Remote Registry Service enables remote users who have the appropriate permissions to modify registry settings on the domain controller. This service is installed and automatically run by default on Windows XP and Windows Server 2003 computers. However, the service’s default configuration only allows Administrators and Backup Operators to access the registry remotely. This service is required for the Microsoft Baseline Security Analyzer (MBSA) utility. MBSA is a tool that allows you to verify which patches are installed on each of the servers in your organization.

If the Remote Registry Service stops, only the registry on the local computer will be able to be modified. If you disable this service, any services that explicitly depend on the service will not start but registry operations on your local computer will not be affected. However, other computers or devices will no longer be able to connect to your local computer’s registry.
Remote Server Manager

The Remote Server Manager service provides the following functionality:

- Holds the Remote Administration alert information.
- Provides an interface to raise, clear, and enumerate Remote Administration alerts.
- Provides an interface to execute Remote Administration tasks.

The Remote Server Manager service is installed and set to automatically start by default on computers that run Windows Server 2003. The service acts as a WMI instance provider for Remote Administration Alert Objects and a WMI method provider for Remote Administration Tasks. The service runs under the Local System account, and requests on the COM interface are only accepted from clients that run under the Administrator or Local System accounts.

If the Remote Server Manager service is configured to Manual, it will start when the next request for Remote Administration Tasks or Remote Administration Alerts is received. If the service stops, it restarts if the Web interface for remote administration is accessed. If you disable this service, any services that explicitly depend on this service will not start. Also, you will lose information about any current Remote Administration Alerts if you disable this service.

Remote Server Monitor

The Remote Server Monitor service monitors critical computer resources and manages optional watchdog timer hardware on remotely managed servers.

If the Remote Server Monitor service stops, it will no longer monitor critical computer resources and the hardware watchdog timer will stop.

Remote Storage Notification

The Remote Storage Notification service notifies the user when a user program attempts to read from or write to files that are only available from secondary storage media. Because of the extended period of time it takes to access a file that has been moved to tape, Remote Storage notifies the user when an attempt to read a migrated file occurs. Also, the service allows the user to cancel the request instead of waiting.

The Remote Storage Notification service is not installed by default on Windows XP or Windows Server 2003. If this service stops, you will not receive additional notification when you try to open offline files, nor will you be able to cancel an operation that involves an offline file.

Remote Storage Server

The Remote Storage Server service stores infrequently used files in secondary storage media. This service allows the Remote Storage subsystem in Windows to notify the user when an offline file has been accessed.

Remote Storage is a hierarchical storage management application that moves data from upper-level storage to lower-level storage. Upper-level storage is commonly known as local storage, or data that is frequently accessed and stored locally on high-performance disks. Lower-level storage is also known as remote storage, or data that is infrequently accessed and stored on less expensive media until it is needed again. Hierarchical storage management reduces storage costs for large quantities of data, but ensures that the data is still accessible.
Chapter 7: System Services

The Remote Storage Server service is installed as part of the Remote Storage Windows component, which must be manually installed. When installed, the service is set to run automatically. If this service stops, files cannot be moved to or retrieved from the secondary storage media.

Removable Storage

The Removable Storage service manages and catalogs removable media and operates automated removable media devices. This service maintains a catalog of information that identifies removable media that are used by your computer, including tapes, and CDs. If the computer also has automated devices to maintain removable media such as a tape autoloader or CD jukebox, the Removable Storage service also automates mount, dismount, and eject media functions. Applications such as Backup and Remote Storage use this service to catalog media and for automation. In summary, this service labels and tracks media and controls library drives, slots, and doors. It also provides drive-cleaning operations.

The Removable Storage service is installed by default on Windows Server 2003 and Windows XP. Its default configuration is to run only when removable storage access is requested by a program on the local computer. If this service stops, applications that depend on it (such as Backup and Remote Storage) will operate more slowly. The Removable Storage service becomes inactive when there is nothing to process. If there are no automated devices attached to the computer, the service will execute only when applications use it. Therefore, it is not necessary to stop the service. When started under these circumstances, the Removable Storage Manager frequently needs to inventory the complete contents of attached autoloaders and jukeboxes, which requires each media item to be mounted in a drive.

Resultant Set of Policy Provider

The Resultant Set of Policy Provider service enables you to connect to a Windows Server 2003 domain controller, access the WMI database for that computer, and simulate Resultant Set of Policy (RSoP) for Group Policy settings. The policy settings are determined for a user or computer that is located in Active Directory. This simulation is commonly referred to as planning mode.

The Resultant Set of Policy Provider service is installed by default on Windows Server 2003 computers, but its startup type is configured to Manual. If this service stops on a domain controller, RSoP Planning Mode simulation will be unavailable on that domain controller. RSoP only needs to run on domain controllers; member servers and workstations do not need to run this service to use the feature.

Routing and Remote Access

The Routing and Remote Access service provides multi-protocol LAN-to-LAN, LAN-to-WAN, VPN, and NAT routing services. This service also provides dial-up and VPN remote access services.

The Routing and Remote Access service replaces the Routing and Remote Access Service (RRAS) and Remote Access Service (RAS) features in Windows NT 4.0. The Routing and Remote Access service is a single, integrated service that terminates connections from either dial-up or VPN clients and provides routing of IP, IPX, and Services for Macintosh. Your server can use this service to function as a remote access server, a VPN server, a gateway, or a branch-office router.
From a routing perspective, the **Routing and Remote Access** service supports the Open Shortest Path First (OSPF) and Routing Information Protocol (RIP) routing protocols, and controls the routing tables for the TCP/IP stack-forwarding engine.

The **Routing and Remote Access** service is installed by default on Windows Server 2003 computers. It is disabled by default. If this service stops, your computer will not be able to accept incoming RAS, VPN, or dial-on-demand connections, and routing protocols will not be received or transmitted.

**SAP Agent**

The **SAP Agent** service advertises network services on an IPX network through the IPX Service Advertising Protocol (SAP). It also forwards advertisements on a multi-homed host. Some features, such as the File and Print Services for NetWare from Microsoft, rely on this service.

The **SAP Agent** service requires installation of the NWLINK IPX/SPX Compatible Transport protocol, and it is not installed or activated by default. If this service is turned off, the referenced features may not function correctly.

**Secondary Logon**

The **Secondary Logon** service allows a user to create processes in the context of different security principals. A common use of this service is by administrators who may log on as restricted users but need administrative privileges to run a specific application. They can use a secondary logon to temporarily run such applications.

Another component of the **Secondary Logon** service is RunAs.exe, which allows you to run programs (*.exe files), saved MMC consoles (*.msc files), shortcuts to programs and saved MMC consoles, and Control Panel items as Administrator while you are logged on to your computer as a member of another group, such as the **Users** group. In Windows 2000, this service was called the **RunAs Service**.

The **Secondary Logon** service is installed and run automatically by default on Windows XP and Windows Server 2003. If the service stops or if you disable it, this type of logon access will be unavailable. Any calls to the **CreateProcessWithLogonW** API will fail. Specifically, if you stop or disable this service, the MMC snap-in that launches applications as other users and the RunAs.exe tool will malfunction.

**Security Accounts Manager**

The **Security Accounts Manager (SAM)** service is a protected subsystem that manages user and group account information. In Windows 2000 and the Windows Server 2003 family, workstation security accounts are stored by the service in the local computer registry, and domain controller security accounts are stored in Active Directory. In Windows NT 4.0, both local and domain security accounts are stored in the registry.

The startup of the **Security Accounts Manager** service signals other services that it is ready to accept requests.

The **Security Accounts Manager** service is present on all versions of Windows XP and Windows Server 2003, and you cannot stop it. If you disable this service, other services in the computer may not start correctly. Do not disable this service.
Security Center

The **Security Center** service provides a central location for computers that run Windows XP with SP2 to manage security-related settings. It is configured to run automatically by default. When it runs, it performs the following tasks:

- Checks whether the **Windows Firewall** service is running and queries specific third-party WMI providers to see if compatible software firewall applications are present and running.

- Queries specific third-party WMI providers to see if compatible antivirus software is installed, whether the software is up-to-date, and whether real-time scanning is turned on.

- Checks the configuration of the **Automatic Updates** service. If the **Automatic Updates** service is turned off or not configured in accordance with the recommended settings, the **Security Center** service will inform the user.

If the **Security Center** service determines that a protected component is missing, incorrectly configured, or out of date, it notifies the user through a logon alert message and icon in the notification area of the taskbar.

If you disable the **Security Center** service, the protected components will continue to function in accordance with their specific configuration settings. However, no centralized monitor service will be provided.

Server

The **Server** service provides RPC support, file, print, and named pipe sharing over the network. It allows local resources to be shared, such as disks and printers, so that other users on the network can access them. It also allows named pipe communication between applications that run on other computers and your computer, which is used to support RPC. Named pipe communication is memory that is reserved for the output of one process to be used as input for another process. The input-acceptance process does not need to be local to the computer. This service is installed and runs automatically by default on Windows XP and Windows Server 2003.

If the **Server** service stops or if you disable it, the computer will not be able to share local files and printers with other computers on the network, and it will not be able to satisfy remote RPC requests.

Shell Hardware Detection

The **Shell Hardware Detection** service monitors and provides notification for AutoPlay hardware events. AutoPlay is a feature that detects content such as pictures, music, or video files on removable media and removable devices. AutoPlay then automatically launches applications to play or display that content, which simplifies the use of specialized peripheral devices such as MP3 players and digital photo readers. The service also makes it easier for users, because they do not need to know beforehand what software applications are needed to access various content types.

AutoPlay supports a variety of media content types and applications. Both independent hardware vendors (IHVs) and independent software vendors (ISVs) can extend this support to include their hardware devices and applications. A user can configure a different AutoPlay action for any combination of pictures, music files, and video.
Media and device types that are supported by AutoPlay include:

- Removable storage media
- Flash media
- PC cards
- External hot-plug USB or 1394 fixed drives
- Supported content types, which include:
  - Pictures (.jpg, .bmp, .gif, and .tif files)
  - Music Files (.mp3 and .wma files)
  - Video (.mpg and .asf files)

The Shell Hardware Detection service is installed and runs automatically by default on Windows XP and Windows Server 2003. If the service stops, the Hardware AutoPlay functionality will not work, the My Computer icons and labels will revert to Windows 2000 functionality, and shell performance will also be affected.

**Simple Mail Transport Protocol (SMTP)**

The Simple Mail Transport Protocol (SMTP) service is an e-mail submission and relay agent. It can accept and queue e-mail messages for remote destinations and establish connections to other computers at specified intervals. Windows domain controllers use the SMTP service for inter-site e-mail-based replication. Also, the Collaboration Data Objects (CDO) for the Windows Server 2003 COM component can use this service to submit and queue outbound e-mail.

The SMTP service is installed and run by default on Windows Server 2003, Web Edition. On Windows XP and other Windows Server 2003 editions, it is an optional component that is not installed by default.

**Simple TCP/IP Services**

The Simple TCP/IP Services service implements support for the following protocols and ports:

- Echo, port 7, RFC 862
- Discard, port 9, RFC 863
- Character Generator, port 19, RFC 864
- Daytime, port 13, RFC 867
- Quote of the Day, port 17, RFC 865

When you enable Simple TCP/IP Services, all five protocols are enabled on all adapters. There is no ability to selectively enable specific services or enable the service on per-adapter basis.

If you stop or disable Simple TCP/IP Services, the rest of the operating system is unaffected. This service must be manually installed. Do not install this service unless you specifically need a computer to support communication with other computers that use the referenced protocols.
Single Instance Storage Groveler

The Single Instance Storage Groveler (SIS) service is an integral component of Remote Installation Services (RIS). This service scans the RIS volume for duplicate files to reduce the overall amount of storage that is required on the volume. If the service finds duplicate files, it copies the original file into single instance storage and leaves a link file in its place. The link file contains information about the original file, such as its current location, size, and attributes. If an image contains duplicate files, those duplicates are copied into the store. As a result, less disk space is required on the RIS server.

The SIS Groveler service has two limitations.

• It cannot act upon any files that are referenced through junction points.
• It cannot be used with any file system except NTFS, which is the only file system supported on RIS servers.

The SIS Groveler service is only present if the Remote Installation Services component has been installed. In that case, it will be started automatically at boot time. If the SIS Groveler service stops, files will no longer be automatically linked in this manner, but the existing linked files will still be accessible. New RIS installation images will consume their full image size and conserve little space. If the SIS Groveler service is no longer needed on the computer, the proper way to discontinue its use is to use the Add/Remove Windows Components tool to remove the Remote Installation Services component, which will disable it.

Smart Card

The Smart Card service manages and controls access to a smart card that is inserted into a smart card reader, which is connected to your computer. The smart card subsystem is based on Personal Computer/Smart Card (PC/SC) Workgroup consortium standards and consists of the Resource Manager component, which manages access to readers and smart cards. To manage these resources, the Resource Manager performs the following functions:

• Identifies and tracks resources.
• Allocates readers and resources across multiple applications.
• Supports transaction primitives to access services that are available on a given card.

The Resource Manager also exposes a subset of the Win32 API to provide applications with access to a Card/Reader Selection user interface (UI). This component allows simple smart card-aware applications to access a card and reader with minimum coding.

The Smart Card service is automatically installed by default on Windows XP and Windows Server 2003 computers. Its startup state is configured to Manual, and the service will be started when an application requests smart card access. If this service stops, your computer will be unable to read smart cards.

SNMP Service

The SNMP Service allows inbound Simple Network Management Protocol (SNMP) requests to be serviced by the local computer. This service includes agents that monitor activity in network devices and report to the network console workstation, and provides a way to manage network hosts such as workstation or server computers, routers, bridges, and hubs from a centrally-located computer that runs network management software. SNMP performs management services through a distributed architecture of management computers and agents.
You can use SNMP to perform the following tasks:

- **Configure remote devices.** Configuration information can be sent to each networked host from the management computer.

- **Monitor network performance.** You can track the speed of processing, network throughput, and collect information about the success of data transmissions.

- **Detect network faults or inappropriate access.** You can configure trigger alarms on network devices when certain events occur. When an alarm is triggered, the device forwards an event message to the management computer. Common types of alarms include a device being shut down and restarted, a link failure being detected on a router, and inappropriate access.

- **Audit network usage.** You can monitor overall network usage to identify user or group access as well as types of usage for network devices and services.

The **SNMP Service** also includes an SNMP agent that allows remote, centralized management of computers that run the following versions of the Windows operating system:

- Windows XP Home Edition
- Windows XP Professional
- Windows 2000 Professional
- Windows 2000 Server
- Windows Server 2003 family

The SNMP agent also allows management of the following services:

- Windows XP or the Windows Server 2003 family and Windows 2000–based WINS
- Windows XP or the Windows Server 2003 family and Windows 2000–based DHCP
- Windows XP or the Windows Server 2003 family and Windows 2000–based Internet Information Services
- LAN Manager

The **SNMP Service** is only installed if you manually install the optional SNMP component through the Windows Components wizard. When installed, the service starts automatically. If the **SNMP Service** stops or if you disable it, the computer will no longer respond to SNMP requests. If the computer is being monitored by network management tools that rely on SNMP, they will no longer be able to collect data from the computer, nor be able to control its functionality through the service.

**SNMP Trap Service**

The **SNMP Trap Service** receives trap messages, which contain information about specific events and are generated by local or remote SNMP agents. The service forwards the messages to SNMP management programs that run on your computer. The **SNMP Service**, when configured for an agent, generates trap messages if any specific events occur, and these messages are sent to a trap destination. For example, an agent can be configured to initiate an authentication trap if an unrecognized management computer sends a request for information. Trap destinations consist of the computer name, the IP address, or IPX address of the management computer. The trap destination must be a network-enabled host that runs SNMP management software. Trap destinations can be configured by a user, but the events, such as computer restarts, that generate trap messages are internally defined by the SNMP agent.

The **SNMP Trap Service** is only installed if you manually install the optional SNMP component through the Windows Components wizard. When installed, the service starts
automatically. If the service stops or if you disable it, SNMP-based programs on the
computer will not receive SNMP trap messages from other computers. If this computer
monitors network devices or server applications with SNMP traps, significant computer
events will be lost.

**Special Administration Console Helper**

You can use the **Special Administration Console Helper** service to perform remote
management tasks on a computer that runs a version of Windows Server 2003 if the
computer's functions are halted because of a **Stop** error message. The Windows
Emergency Management Services component supports two out-of-band console
interfaces: the Special Administration Console (SAC) and !SAC, which offers a subset of
SAC commands for use when the server has been halted.

Both the SAC and !SAC components accept input and send output through the out-of-
band port. SAC is a separate entity from both !SAC and the Windows Server 2003 family
command-line environments. After a specific failure point is reached, Emergency
Management Services components determine when the shift should be made from SAC
to !SAC. !SAC becomes available automatically if SAC fails to load or does not function.

The **Special Administration Console Helper** service allows you to create inbound
communication channels through the command prompt. This service is only installed on
Windows Server 2003 computers, and only when you enable the Emergency
Management Services functionality as described in the Windows Server 2003
documentation.

If the **Special Administration Console Helper** service stops, SAC services will no
longer be available.

**SQLAgent$* (* UDDI or WebDB)**

The **SQLAgent$* (* UDDI or WebDB)** service is a job scheduler and monitoring service.
It also moves information between SQL servers and is used heavily for backups and
replication. These services are not installed or active by default.

If the **SQLAgent$* (* UDDI or WebDB)** service stops, SQL replication will not occur.
Also, there will be a disruption of all scheduled jobs, alert/event monitoring and auto
restart of the SQL Server service.

**SSDP Discovery Service**

The Universal Plug and Play host service that is included with Windows XP supports
peer-to-peer Plug and Play functionality for network devices. The UPnP specification is
designed to simplify device and network service installation and management. The
Universal Plug and Play host service uses the Simple Service Discovery Protocol (SSDP)
to locate and identify UPnP network devices.

The **SSDP Discovery Service** is installed and configured to **Manual** on Windows XP
computers. The service is only started when the computer attempts to locate and
configure UPnP devices. If you disable this service, the computer will be unable to find
UPnP devices on the network and the Universal Plug and Play host service will not be
able to find and interact with UPnP devices.
**System Event Notification**

The **System Event Notification** (SENS) service monitors and tracks computer events such as Windows logon network and power events. It also notifies **COM+ Event System** subscribers of these events. This service is installed by default and runs automatically under Windows XP and Windows Server 2003.

If the **System Event Notification** service stops, subscribers to the **COM+ Event System** service will not receive event notifications and the following problems will occur:

- Win32 APIs IsNetworkAlive() and IsDestinationReachable() will not work. These APIs are mostly used by mobile applications on laptops.
- ISens* interfaces will not work. SENS logon/logoff notifications will fail.
- SyncMgr (Mobsync.exe) will not work properly. It depends on connectivity information and also on Network Connect/Disconnect and Logon/Logoff notifications from SENS.
- The COM+ EventSystem will fail when it tries to notify SENS of some events.
- The **Volume Shadow Copy** service will not load properly, which will cause the Windows Backup API to fail.

**System Restore Service**

The **System Restore Service** provides Windows XP users with the ability to take snapshots of their computer configuration and save them as a series of restore points. These restore points can be used as fail-safe configurations after an unsuccessful attempt to install or upgrade a device driver or application.

The **System Restore Service** is enabled by default and will automatically create a new restore point just before major changes are made to the computer, such as the installation of new device drivers, updates, and applications. Automatic restore points are also created on a daily basis, although this schedule can be further modified.

If you disable the **System Restore Service**, the automatic computer restore functionality will no longer be available and no restore points will be created automatically or manually.

**Task Scheduler**

The **Task Scheduler** service enables you to configure and schedule automated tasks on your computer. The service monitors whatever criteria you choose and carries out the task when the criteria have been met.

You can use the **Task Scheduler** service’s GUI to perform the following tasks:

- Create work items (currently the only type of work item that is available is tasks).
- Schedule tasks to run at specific times or when a specific event occurs. For example, you can have the computer run ScanDisk at 7:00 P.M. every Sunday.
- Change the schedule for a task.
- Customize how tasks are run.
- Stop a scheduled task.

You can start the **Task Scheduler** service from the MMC Services snap-in under Computer Management or configure it to start automatically. By default, the **Task Scheduler** service is installed on Windows XP and Windows Server 2003 computers. It
Chapter 7: System Services

can be accessed from the Task Scheduler GUI, through the Task Scheduler API as described in the SDK, or from the SchTasks.exe utility.

If the **Task Scheduler** service stops, scheduled tasks will not run at their scheduled times or intervals. Also, this service is needed for Windows Backup and backup applications that rely upon the Windows Backup API. If there are not any jobs listed in the `%System Root%\Tasks` folder, there will be minimal effect if you stop the service. Otherwise, jobs that are required to run will be unable to start. The Systems Management Server Software Update Services Feature Pack will fail if the **Task Scheduler** service is unavailable. Also, scheduled backups will fail to run if the **Task Scheduler** service stops.

**TCP/IP NetBIOS Helper Service**

The **TCP/IP NetBIOS Helper Service** provides support for the NetBIOS over TCP/IP (NetBT) service and NetBIOS name resolution for clients on your network. It enables users to share files, print, and log on to the network. Specifically, the service performs DNS name resolution and pings a set of IP addresses that return a list of accessible IP addresses to provide support for the NetBT service.

The **TCP/IP NetBIOS Helper Service** is installed and started automatically by default on Windows Server 2003 and Windows XP. If this service stops or if you disable it, NetBT, Redirector (RDR), Server (SRV), **Net Logon** and **Messenger** service clients might not be able to share files, printers and log on to computers. For example, domain-based Group Policy will no longer function.

**TCP/IP Print Server**

The **TCP/IP Print Server** service enables TCP/IP-based printing through the Line Printer Daemon protocol. The Line Printer Daemon Service (LPDSVC) on the server receives documents from native Line Printer Remote (LPR) utilities that run on UNIX computers.

The **TCP/IP Print Server** service is an optional component that must be separately installed from the Windows Components wizard. If this service stops, TCP/IP-based printing will be unavailable.

**Telephony**

The **Telephony** service provides TAPI support for programs that control telephony devices, as well as IP-based voice connections on the local computer and through LAN servers that also run the service. The service enables applications to act as clients to telephony equipment such as Private Branch Exchanges (PBXs), telephones, and modems. It supports the TAPI under which different wire protocols that communicate with telephony equipment are supported. These protocols are implemented in Telephony Service Providers (TSPs).

The **Telephony** service is installed by default on Windows XP and Windows Server 2003, and its startup state is configured to **Manual**. Applications that require TAPI service may start it. If the **Telephony** service stops or if you disable it, any services that explicitly depend on it (such as modem support) will not start. You cannot stop the service if there is another dependent service currently active, such as RAS. If you stop the service when no dependent services are active, it will restart when any application makes an initialization call to the TAPI interface.
**Telnet**

The Telnet service for Windows provides ASCII terminal sessions to Telnet clients. It supports two types of authentication and supports four types of terminals: American National Standards Institute (ANSI), VT-100, VT-52, and VTNT.

The Telnet service also allows a remote user to log on to a computer and run console programs from the command line. A computer that runs the Telnet service can support connections from various TCP/IP Telnet clients, including UNIX-based and Windows-based computers. The Telnet service is installed on Windows XP and Windows Server 2003 computers by default, but it is disabled. For upgrade installations, the startup type of the Telnet service in the previous version of Windows is preserved.

If the Telnet service stops, remote user access to programs will be unavailable through the Telnet client, remote users will be unable to connect through the Telnet protocol, and users will not be able to connect to the computer or run console-based applications.

**Terminal Services**

The Terminal Services service provides a multi-session environment that allows client devices to interact with virtual Windows desktop sessions and Windows-based programs that run on a server.

By default, the Terminal Services service is installed in remote administration mode on Windows Server 2003 computers. To install Terminal Services in application mode, use Configure Your Server or Add/Remove Windows Components to change the Terminal Services mode. For Windows Server 2003 computers, this service is required if you wish to use Remote Desktop. On Windows XP, it is required if you wish to use Fast User Switching, Remote Desktop, and Remote Assistance. On both versions of Windows, this service is installed by default, with a startup type of Manual.

If the Terminal Services system service stops or if you disable it, your computer might become unreliable and Remote Assistance will no longer be available. To prevent remote use of your computer, clear the Allow Remote Assistance and Allow Remote Desktop checkboxes on the Remote tab of the System Properties property sheet.

**Terminal Services Licensing**

The Terminal Services Licensing service installs a license server and provides registered client licenses when connections are made to a Terminal Server. The Terminal Services Licensing service is a low-impact service that stores the client licenses that have been issued for a Terminal Server and then tracks the licenses that have been issued to client computers or terminals. This service will only be present and is only required for servers on which the Terminal Services service is installed in application mode.

If the Terminal Services Licensing service is turned off, the server will be unavailable to issue Terminal Server licenses to clients when they request them. If another license server is discoverable on a domain controller in the forest, the requesting Terminal Server will attempt to use it.

**Terminal Services Session Directory**

The Terminal Services Session Directory service provides a multi-session environment that allows client devices to access a virtual Windows desktop session and Windows-based programs that run on Windows Server 2003.
The **Terminal Services Session Directory** service allows clusters of load-balanced Terminal Servers to properly route a user’s connection request to the server where the user already has an active session. The Windows Network Load Balancing service pools the processing resources of several servers that use the TCP/IP networking protocol. You can use the Windows Network Load Balancing service with a cluster of Terminal Servers to provide a single Terminal Server access point to users while distributing sessions across multiple servers.

The **Terminal Services Session Directory** service keeps track of disconnected sessions on the cluster, and ensures that users are reconnected to those sessions. This service is installed on Windows Server 2003 computers that have the Terminal Services component installed, but the service is disabled by default. Microsoft recommends that the **Terminal Services Session Directory** service be installed on a server that is not a Terminal Server.

If the **Terminal Services Session Directory** service stops, connection requests will be routed to the first available server, regardless of whether they have an active session elsewhere in the cluster.

### Themes

The **Themes** service provides user experience theme-management services. The **Themes** service provides rendering support for the new Windows XP GUI. A desktop theme is a predefined set of icons, fonts, colors, sounds, and other elements that give the computer desktop a unified and distinctive look. You can switch themes, create your own theme by changing a theme and then saving it with a new name, or restore the traditional Windows Classic look as your theme. On Windows XP computers, the **Themes** service is set to start automatically. On Windows Server 2003 computers, it is disabled.

If the **Themes** service stops or if you disable it, the new Windows XP visual style—windows, buttons, scrollbars and other controls—will revert to the Windows Classic visual style.

### Trivial FTP Daemon

The **Trivial FTP Daemon** service (TFTP) does not require a user name or password and is an integral part of the Remote Installation Services (RIS) for Windows Server 2003. The service implements support for the TFTP protocol that is defined by the following RFCs:

- RFC 1350 – TFTP
- RFC 2347 – Option extension
- RFC 2348 – Block size option
- RFC 2349 – Timeout interval, and transfer size options

A Remote Installation server uses the **Trivial FTP Daemon** service to download the initial files that are required for the remote installation process to begin. The most common file that is downloaded to the client through this service is Startrom.com, which bootstraps the client computer. If the user presses F12 when prompted, the Client Installation Wizard is downloaded to begin the remote installation process.

The **Trivial FTP Daemon** is not installed by default. If this service stops or if you disable it, client computers that request RIS from this server will fail to install. The correct way to disable this service is to uninstall RIS.
Uninterruptible Power Supply

The Uninterruptible Power Supply service manages an uninterruptible power supply (UPS) that is connected to your computer by a serial port. This service is installed by default on Windows XP and Windows Server 2003, but its startup type is configured to Manual.

If the Uninterruptible Power Supply service stops or if you disable it, communications with the UPS will be lost. If there is a loss of power, the UPS may not be able to safely shut down the computer, which could result in loss of data.

Universal Plug and Play Device Host

The Universal Plug and Play Device Host service supports peer-to-peer Universal Plug and Play (UPnP) functionality for network devices. The UPnP specification is designed to simplify device and network service installation and management. UPnP accomplishes device and service discovery and control through driver-less, standards–based protocol mechanisms.

UPnP devices can automatically configure network addresses, announce their presence on a network subnet, and enable the exchange of device and service descriptions. When the Universal Plug and Play Device Host service is installed, a Windows XP computer can act as a UPnP control point to discover and control the devices through a Web or application interface. This service is installed by default on Windows XP computers and is configured to Manual.

Upload Manager

The Upload Manager service manages the synchronous and asynchronous file transfers between client computers and servers on the network. Driver data is anonymously uploaded from customer computers to Microsoft and then used to help users find the drivers that are required for their computers. The Microsoft Driver Feedback Server requests the client's permission to upload the computer's hardware profile and then search the Internet for information about how to obtain the appropriate driver or get support from Microsoft or an appropriate third party.

Information that is uploaded from your computer to find driver information will include the hardware identification numbers for the device, the time the Windows Hardware Wizard finished, and an ID for the Windows operating system on your computer. The computer information that is uploaded cannot be tracked to a user, computer, organization, IP address, or any other source information.

The collected data is used to track which devices do not have easily obtainable drivers. If additional device driver information exists, it will be available after the device identification number is uploaded. If additional driver information is not available, Microsoft will record the device's identification number and work with hardware vendors to increase the availability of device drivers for Windows or provide information about driver availability and device support.

The Upload Manager service is installed by default and configured to Manual on Windows Server 2003 computers. If this service stops, synchronous and asynchronous file transfers between clients and servers on the network will not occur.
Virtual Disk Service

The Virtual Disk Service (VDS) provides a single interface to manage block storage virtualization, whether it is done in operating system software, redundant array of independent disks (RAID) storage hardware subsystems, or other virtualization engines.

The Virtual Disk Service provides a vendor-neutral and technology-neutral interface to manage logical volumes (software) and logical units (hardware). You can use this interface to manage bind operations, performance monitoring, topology discovery and tracking, volume status, and fault tracking.

Do not confuse virtual disks with snapshots. Unlike the Volume Shadow Copy Service, the Virtual Disk Service does not coordinate with applications or the file system, and the data that is contained on a volume will not be synchronized before a volume or disk configuration operation. You can use the Virtual Disk Service to configure a mirror plex, but a snapshot provider is necessary to perform the coordination when removing the plex and surfacing the snapshot. That use is outside the scope of this document with two exceptions:

- The Virtual Disk Service coordinates with the file system before it extends or shrinks volumes.
- Full copy snapshots appear as plexes to the Virtual Disk Service.

The Virtual Disk Service is installed and configured to Manual on Windows Server 2003 computers. The service is only started when an application attempts to use VDS services. If it stops, VDS services will no longer be available.

Volume Shadow Copy

The Volume Shadow Copy service manages and implements volume shadow copies, which are used for backup and other purposes. The service manages the volume snapshots. When a backup application attempts to start a backup with the new snapshots infrastructure, the backup application determines the number of writers that are currently active on the service and then queries each writer to gather the required metadata. The backup application can then collect the volumes that require a shadow copy to ensure a successful backup session. The volumes are presented to the shadow copy coordinator and a shadow copy is created. The shadow copy creates volumes that match the original volumes at the shadow copy point of time.

The Volume Shadow Copy service is installed on Windows XP and Windows Server 2003 computers, and its startup type is configured to Manual. While the service is stopped, shadow copies will be unavailable for backup and the backup process might not succeed. Specifically, the Volume Shadow Copy service is needed for Windows Backup and backup applications that rely upon the Windows Backup API.

WebClient

The WebClient service allows Win32 applications to access documents on the Internet. The service extends the network capability of Windows; it allows standard Win32 applications to create, read, and write files on Internet file servers through the use of WebDAV, a file-access protocol that is described in XML and uses HTTP for communication. Because it uses standard HTTP, WebDAV runs over existing Internet infrastructure, such as firewalls and routers.

The WebClient service is installed on both Windows XP and Windows Server 2003. On Windows XP, the service starts automatically. On Windows Server 2003, the service is disabled. If the WebClient service stops, users of the computer will not be able to use the
Web Publishing Wizard to publish data to Internet locations that use the WebDAV protocol.

**Web Element Manager**

The **Web Element Manager** service is only installed on Windows Server 2003, Web Edition. It serves Web user interface elements for the Administration Web site at port 8098, which determine the following information:

- Tabs to display on the Administration Web site
- Remote administration tasks that are available to the Administrator
- Table of contents
- Help topics
- Remote administration alerts that can be displayed

To remotely manage a server, an administrator can connect to the server at https://<servername>:8098. When this Web site receives a connection, the default Active Server Pages (ASP) code queries the **Web Element Manager** service for each of the referenced types of information. After all the information has been collected, the appropriate Web page is displayed to the administrator.

The **Web Element Manager** service loads all the information at startup time, and the client—the ASP code, in this scenario—requests the Web user interface elements through a COM interface. The service runs under the Local System account and requests on the COM interface are only accepted from clients that run under the Administrator or Local System accounts. If the service stops or is configured to Manual, it will start when it receives the next request for Web user interface elements.

The **Web Element Manager** service is automatically restarted when the Web interface for remote administration is accessed. If you disable this service, any services that explicitly depend on this service will not start and the Remote Administration Tools Web user interface for server administration will not function properly.

**Windows Audio**

The **Windows Audio** service provides support for sound and related Windows Audio event functions. This service manages Plug and Play compatible events for audio devices such as sound cards and global audio effects (GFX) for Windows audio application program interfaces. Examples of GFXs are equalization (EQ), bass enhancement, and speaker correction. The service loads, unloads, and saves/restores state for the GFXs on a per-session basis.

Through the Multimedia control panel, users can accomplish the following:

- Enable or disable a GFX.
- Select among several GFX filters if more than one GFX is available that is designed for the specific audio hardware. A GFX driver's INF file specifies the target hardware for the GFX.


You cannot stop the **Windows Audio** service after it is started. If you disable this service, audio functionality may be affected, including the inability to hear sound or process GFXs.
Windows Firewall /Internet Connection Sharing

The Windows Firewall/Internet Connection Sharing (ICS) service provides network address translation (NAT), address and name resolution, and/or intrusion-prevention services for all computers on a home or small-office network through a dial-up or broadband connection.

When this service is enabled, the computer becomes an “Internet gateway” on the network. It allows other client computers to share one connection to the Internet, share files, and use the same printers. This service has a location-aware Group Policy.

This service was previously called Internet Connection Sharing in Windows 2000 and Windows XP Service Pack 1. It was not included in the original release of Windows Server 2003.

The Windows Firewall/Internet Connection Sharing service is a default service that installs and starts automatically on Windows XP computers. The service also installs on Windows Server 2003 computers by default, but it is configured to Disabled.

If the Windows Firewall/Internet Connection Sharing service stops, network services such as Internet sharing, name resolution, address resolution, and/or intrusion prevention will be unavailable. Clients on the network might not be able to access the Internet and their IP addresses will expire, which will cause some clients to use Automatic Private IP Addressing (APIPA) for peer-to-peer network connectivity.

Windows Image Acquisition (WIA)

The Windows Image Acquisition (WIA) service provides image acquisition services for scanners and cameras.

Windows Server 2003 supports still-image devices through this service, which uses the Windows Driver Model (WDM) architecture. The service provides robust communication between applications and image-capture devices, and allows you to capture images efficiently and transfer them to your computer to be edited and used. The service is needed to capture events that are generated by imaging devices.

The Windows Image Acquisition (WIA) service supports Small Computer System Interface (SCSI), IEEE 1394, USB, and serial digital still-image devices. Support for infrared, parallel, and serial still-image devices is provided by the existing infrared, parallel, and serial interfaces. Image scanners and digital cameras are examples of still-image devices. The service also supports Microsoft DirectShow®–based WebCams and digital video (DV) camcorders to capture frames from video.

The Windows Image Acquisition (WIA) service is installed and configured to Manual on Windows XP, and it is installed and disabled by default on Windows Server 2003 computers. If the service stops, events from imaging devices are not captured and processed. The service will restart automatically at startup if there is a WIA device installed. Also, it restarts any time that a WIA-enabled application is launched.

Windows Installer

The Windows Installer service manages the installation and removal of applications. It applies a set of centrally defined setup rules during the installation process that specify how applications are installed and configured. You can also use this service to modify, repair, or remove existing applications. The Windows Installer technology consists of the Windows Installer service for the Windows operating systems and the package (.msi) file format that is used to hold application setup and installation information.
The **Windows Installer** service is not only an installation program, but it is also an extensible software management system. It manages the installation, addition, and deletion of software components, monitors file resiliency, and maintains basic disaster recovery by way of rollbacks. It also supports the installation and operation of software from multiple sources, and can be customized by developers who want to install custom applications.

By default, the **Windows Installer** service is installed and configured to **Manual** on both Windows XP and Windows Server 2003 computers. Applications that use the installer start the service. If this service stops, applications that use it will not be able to be installed, removed, repaired, or modified. Also, a number of applications make use of this service when they are active, and they might not be able to execute.

### Windows Internet Name Service (WINS)

The **Windows Internet Name Service (WINS)** enables NetBIOS name resolution. The presence of WINS servers is crucial to locate network resources that are identified by their NetBIOS names. WINS servers are required unless all domains have been upgraded to Active Directory, and all computers on the network run Windows 2000 Server or subsequent versions of the Windows operating system.

If you stop this service, the following changes in functionality will occur:

- Windows NT 4.0 domains and domain controllers will not be able to be located.
- Windows 2000 or Windows Server 2003 Active Directory domains and domain controllers will not be able to be located from Windows NT 4.0 clients.
- NetBIOS name resolution will fail, unless the device whose name must be resolved is on the same subnet as the device that attempts name resolution. The device must be configured to attempt NetBIOS name resolution through broadcasts.

The **WINS** service will only be present on Windows Server 2003 computers that have been configured to act in the WINS server role.

### Windows Management Instrumentation

The **Windows Management Instrumentation** (WMI) service provides a common interface and object model to access management information about operating systems, devices, applications, and services. WMI is an infrastructure that provides the ability to build management applications and instrumentation, and is included as part of the current generation of Microsoft operating systems.

The WMI infrastructure is a Microsoft Windows operating system component that moves and stores information about managed objects. It is composed of two components: the **Windows Management Instrumentation** service and the WMI repository. The service acts as an intermediary between the providers, management applications, and the WMI repository, and places information from a provider into the WMI repository. The service also accesses the WMI repository in response to queries and instructions from management applications. Finally, the service can pass information directly between a provider and a management application. In contrast, the WMI repository acts as a storage area for information from the various providers.

The **Windows Management Instrumentation** service provides access to the management data through a number of interfaces, including COM API, scripts and command line interfaces. It is compatible with previous management interfaces and protocols, such as Simple Network Management Protocol (SNMP). The service installs and runs automatically on Windows XP and Windows Server 2003 computers. If the service stops, most Windows–based software will not function properly.
**Windows Management Instrumentation Driver Extensions**

The Windows Management Instrumentation Driver Extensions service monitors all drivers and event trace providers that are configured to publish WMI or event trace information. By default, this service is installed on Windows XP and Windows Server 2003 and configured to Manual.

**Windows Media Services**

The Windows Media Services service provides streaming media services over IP-based networks. These services replace the four separate services that comprised Windows Media Services versions 4.0 and 4.1:

- Windows Media Monitor service
- Windows Media Program service
- Windows Media Station service
- Windows Media Unicast service


The Windows Media Service platform is compliant with the following industry standards:

- WMI for server event notification and messaging
- SNMP for networking components
- XML, Synchronized Multimedia Integration Language (SMIL) 2.0, and the Document Object Model (DOM) for playlist implementation
- Moving Picture Experts Group (MPEG) 1 and 2 for audio and video formats

Most streaming media scenarios use the core components that are installed with Windows Media Services. However, more advanced scenarios may require you to incorporate some custom programming and integration work. For developers and systems integrators, the Windows Media Services SDK provides access to all elements of the server through a combination of plug-ins, a fully documented object model, and a rich set of external event notifications, all of which are designed to be easily customizable.

Windows Media Services is an optional service that must be separately installed on Windows Server 2003 computers. If this service stops or if you disable it, streaming media services might be unavailable.

**Windows System Resource Manager**

The Windows System Resource Manager (WSRM) service is an optional tool to help customers deploy applications into consolidation scenarios. It provides policy-based management of CPU and memory consumption of processes that run on a single instance of an operating system. Planned scenarios include multiple heterogeneous server applications, multiple Terminal Services users, multiple SQL server instances, and multiple IIS V6 application pools or Exchange and IIS V6 together on the same computer.
The primary option for CPU management is bandwidth targets, which are expressed as a percentage of CPU usage. To maintain targets, process priorities are dynamically monitored and adjusted. The WSRM service also provides affinity management, which is provided through per-process APIs for hard affinity.

Memory management options include working set limits and committed memory maximum applied on a per-process basis. Working set limits are defined in policy and applied by WSRM through a kernel API. Subsequently, the kernel memory manager will page the process as necessary to apply and maintain the limits on working set size. Committed memory is simply monitored against an upper limit. When the upper limit is exceeded, the process is terminated or an event is logged—at the user’s discretion.

Additional features include full calendar features to schedule desired policies, sophisticated pattern matching to identify processes at runtime, WSRM-specific counters, and a basic job accounting system.

The WSRM service is implemented as an option and runs on versions of the Windows operating system that were released after Windows 2000 Service Pack 3. The server components may be installed on Windows Server 2003, Datacenter Edition and Windows Server 2003, Enterprise Edition (plus the x64 versions of these editions). The WSRM client must be installed on each managed computer. For administration of the service, an MMC snap-in and command line programs are provided. These client pieces may be installed and run on any Windows 2000 or Windows XP Professional computer or the Windows .NET system. The service may only be installed and run on .NET Datacenter and .NET Enterprise. These SKUs are enforced at install time and runtime.

**Windows Time**

The Windows Time service maintains date and time synchronization on all computers on a Microsoft Windows network. It uses the Network Time Protocol (NTP) to synchronize computer clocks so that an accurate clock value, or timestamp, can be assigned to network validation and resource access requests. The implementation of NTP and the integration of time providers make Windows Time a reliable and scalable time service for administrators. For computers that are not joined to a domain, you can configure the Windows Time service to synchronize time with an external time source. If this service is turned off, the time setting for local computers will not be synchronized with any time service in the Windows domain or external time service.

If the Windows Time service stops or if you disable it, date and time synchronization will be unavailable in the forest or from an external NTP server. There are two possible scenarios:

- If you stop the Windows Time service on a workstation, the workstation will not be able to synchronize its time with another source but no other external server will be affected.
- If you stop the Windows Time service on a domain controller, the same effect as in the previous scenario will apply but domain members will also be unable to synchronize time with it. This inability to synchronize may adversely affect time synchronization in the organization.

By default, the Windows Time service is installed and started automatically on Windows XP and Windows Server 2003 computers.

WinHTTP Web Proxy Auto-Discovery Service

The WinHTTP Web Proxy Auto-Discovery Service implements the Web Proxy Auto-Discovery (WPAD) protocol for Windows HTTP Services (WinHTTP). WPAD is a protocol that enables an HTTP client to automatically discover a proxy configuration.

If the WinHTTP Web Proxy Auto-Discovery Service stops or if you disable it, the WPAD protocol will be executed within the HTTP client's process instead of an external service process and there would be no loss of functionality. This service is installed on Windows Server 2003 computers by default and its startup type is configured to Manual.

Wireless Configuration

The Wireless Configuration service enables automatic configuration for IEEE 802.11 wireless adapters for wireless communications. Microsoft has worked with 802.11 network interface card (NIC) vendors to automate the NIC configuration process, which associates the NIC with an available network and improves the wireless roaming experience on Windows.

Note: The Wireless Configuration service is labeled as the Wireless Zero Configuration service in Windows XP.

The wireless NIC and its Network Driver Interface Specification (NDIS) driver need to do little more than provide support for a few new NDIS Object Identifiers (OIDs) that are used to query and set device and driver behavior. The NIC will scan for available networks and pass the information to Windows. The Wireless Configuration service configures the NIC for an available network. When two networks cover the same area, the user can configure a preferred network order and the computer will try each network in order until it finds an active one. It is also possible to limit association to only the configured, preferred networks.

The Wireless Configuration service installs and starts automatically on Windows Server 2003 and Windows XP computers (with the exception of Windows Server 2003, Web Edition, which configures it to Manual). If this service stops, automatic wireless configuration will be unavailable.

WMI Performance Adapter

The WMI Performance Adapter service provides performance library information from WMI High Performance providers. Applications and services that need to provide performance counters today can do so in two ways: they can write a WMI High Performance provider or write a performance library. Consumers of high performance data also have two ways to request performance data: through WMI or through the Performance Data Helper (PDH) APIs. There are mechanisms in place that allow the two models to interact, so that clients that access counters through each model can still see the counters provided by the other model. The Reverse Adapter is one of those mechanisms.

The WMI Performance Adapter service transforms performance counters that are supplied by WMI High Performance providers into counters that can be consumed by PDH through the Reverse Adapter Performance Library. This approach provides PDH clients such as Sysmon with the ability to consume performance counters from any WMI High Performance providers on the computer.

Although it is installed by default on Windows XP and Windows Server 2003, the WMI Performance Adapter service is a manual service; it does not run by default. It runs on demand when a performance client such as Sysmon uses PDH to query performance data. After the client disconnects, the service stops.
If the **WMI Performance Adapter** service stops, WMI performance counters will be unavailable.

**Workstation**

The **Workstation** service is installed and run automatically on Windows XP and Windows Server 2003. This service creates and maintains client network connections and communications. The **Workstation** service is a user-mode wrapper for the Microsoft Networks redirector. It loads and performs configuration functions for the redirector, supports network connections to remote servers, supports the WNet APIs, and furnishes redirector statistics.

If the **Workstation** service stops, clients will not be able to establish connections to remote servers or access files through named pipes. Clients and programs will note be able to access files and printers on other remote computers, but TCP/HTTP connectivity is not affected. Internet browsing and Web Client access will still work.

**World Wide Web Publishing Service**

The **World Wide Web Publishing Service** provides Web connectivity and administration of Web sites through the MMC IIS snap-in. The service provides HTTP services for applications on the Windows platform and contains a process manager and a configuration manager. The process manager controls the processes in which custom applications and simple Web sites reside. The configuration manager reads the stored computer configuration and ensures that Windows is configured to route HTTP requests to the appropriate application pools or operating system processes.

This service can monitor the processes that house custom applications and provide recycling services for these applications. Recycling is a configuration property of an application pool and can be done on the basis of memory limits, request limits, processing time, or time of day. The service will queue HTTP requests if custom applications stop responding, and will also attempt to restart custom applications.

This service is an optional component that may be installed on Windows Server 2003 or Windows XP as part of the IIS package. If the **World Wide Web Publishing Service** stops, the Windows Server 2003 operating system will not be able to serve any form of Web request.
More Information

The following links provide additional information about some of the settings that are discussed in this chapter:

• A detailed description of how to configure and lock down clusters of Windows servers is beyond the scope of this guide. However, a great source of guidance is the Microsoft Knowledge Base article 891597, “How to apply more restrictive security settings on a Windows Server 2003–based cluster server” at http://support.microsoft.com/kb/891597.

• The Windows Server 2003 Security Configuration Wizard (SCW) includes a configuration database with descriptions and information about the services available in Windows Server 2003 and many other Microsoft server products. To browse this database, you can install the SCW component on any Windows Server 2003 computer and launch the SCW.

• A list of many Windows Server 2003 services and related network port information is available in the Microsoft Knowledge Base article “Service overview and network port requirements for the Windows Server system” at http://support.microsoft.com/kb/832017.


• For more information about how to secure Terminal Services, see “Securing Windows 2000 Terminal Services.” The information in this article is also relevant to Windows Server 2003, and is available at www.microsoft.com/technet/prodtechnol/win2kts/maintain/optimize/secw2kts.mspx.


• For more information about how to restore default security settings locally, see Microsoft Knowledge Base article “How to Reset Security Settings Back to the Defaults” at http://support.microsoft.com/?scid=313222.

• For more information about how to restore default security settings in the built-in domain Group Policy objects, see Microsoft Knowledge Base Article “How to Reset User Rights in the Default Domain Group Policy in Windows Server 2003” at http://support.microsoft.com/?scid=324800.
Software Restriction Policies

Software restriction policies are a new feature in Microsoft® Windows® XP and Microsoft Windows Server™ 2003. They provide a policy-driven system to specify which programs are allowed to execute and which are not.

The Threat of Malicious Software

The increased use of networks and the Internet in daily business computing means that it is more likely than ever that an organization's users will encounter malware (malicious software). Software restriction policies can help organizations protect themselves because they provide another layer of defense against viruses, Trojans, and other types of malicious code.

Vulnerability

People use computer networks to collaborate in increasingly sophisticated ways; they use e-mail, instant messaging, and peer-to-peer applications. As these collaboration opportunities increase, so does the risk from viruses, worms, and other forms of malware. It is important to remember that e-mail and instant messaging can transport unsolicited hostile code, and that hostile code can take many forms—from native Windows executable (.exe) files, to macros in word processing (.doc) documents, to script (.vbs) files.

Viruses and worms are often transmitted in e-mail messages, and they frequently include social engineering techniques that trick users and cause them to perform an action that activates the malicious code. The sheer number and variety of forms that code can take makes it difficult for users to know what is safe to run and what is not. When activated, malicious code can damage content on a hard disk, flood a network with requests to cause a DoS attack, send confidential information to the Internet, or compromise the security of a computer.

Countermeasure

Create a sound design for software restriction policies on end-user computers in your organization, and then thoroughly test the policies in a lab before you deploy them into a production environment.
**Potential Impact**

A flawed software restriction policy implementation can disable necessary applications or allow hostile applications to execute. Therefore, it is important that organizations dedicate sufficient resources to manage and troubleshoot the implementation of such policies.

**Note:** Although software restriction policies are an important tool that can enhance the security of computers, they are not a replacement for other security measures such as antivirus programs, firewalls, and restrictive access control lists (ACLs).

**More Information**

The following links provide additional information about designing and using software restriction policies:


Windows XP and Windows Server 2003 Administrative Templates

The Administrative Template sections of Group Policy include registry–based settings that govern the behavior and appearance of the computers in your environment. These settings also govern the behavior of operating system components and applications. There are hundreds of these settings available for you to configure, and you can import additional .adm files to make more settings available.

This chapter lists the Administrative Template settings that are under the Computer Configuration node of the Group Policy that is defined in this guide as well as those that are under the User Configuration node. This chapter does not examine every setting that is available in the Administrative Templates for Microsoft® Windows® XP and Microsoft Windows Server™ 2003. However, this chapter does provide guidance for all settings that relate to security on computers that run these operating systems. Some settings that are not covered are specific to the following: Application Compatibility, Task Scheduler, Windows Installer, Windows Messenger, and Windows Media® Player.

Previous versions of this guide contained information about the Administrative Templates for Office XP. Microsoft Office 2003 contains a large number of new features and changes to the Administrative Templates that ship with the product. For more information about these changes, see the "More Information" section at the end of this chapter.
Computer Configuration Settings

The following configuration settings apply to computers that are members of an Active Directory® directory service domain. Information about user configuration settings is provided later in this chapter.

NetMeeting

Microsoft NetMeeting® allows users to conduct virtual meetings across the network in your organization. You can configure the NetMeeting Group Policy settings in the following location within the Group Policy Object Editor:

- Computer Configuration\Administrative Templates\Windows Components\NetMeeting

Disable remote Desktop Sharing

This policy setting allows you to disable the remote desktop sharing feature of NetMeeting. You can enable this policy setting so that users cannot configure NetMeeting to automatically answer inbound calls and allow remote control of the local desktop.

The possible values for the Disable remote Desktop Sharing setting are:

- Enabled
- Disabled
- Not Configured

Vulnerability

When this policy setting is enabled, users will not be able to use the remote desktop sharing feature of NetMeeting.

Countermeasure

Configure the Disable remote Desktop Sharing setting to Enabled.

Potential 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.

Internet Explorer Computer Settings

Microsoft Internet Explorer is the Web browser that is included with Windows XP and Windows Server 2003, and you can manage many of its features through Group Policy. You can configure the Internet Explorer Computer Group Policy settings in the following location within the Group Policy Object Editor:

- Computer Configuration\Administrative Templates\Windows Components\Internet Explorer
Disable Automatic Install of Internet Explorer components

This policy setting allows you to prevent the automatic download of components through Internet Explorer when users browse to Web sites that require the components to fully function. If you disable or do not configure this policy setting, users will be prompted to download and install components each time they visit Web sites that use them. This policy setting is intended to help the administrator control which components the user may install.

The possible values for the Disable Automatic Install of Internet Explorer components setting are:

- Enabled
- Disabled
- Not Configured

Vulnerability

Malicious Web site operators can host components that contain hostile code. Users in your organization could inadvertently download this code and run it on the computers in your environment, which could expose confidential data, cause data loss, and create instability.

Countermeasure

Configure the Disable Automatic Install of Internet Explorer components setting to Enabled.

Potential Impact

Internet Explorer will be unable to automatically download components when users browse to Web sites that need them.

Disable Periodic Check for Internet Explorer software updates

If you enable this policy setting, Internet Explorer will not be able to determine whether a later browser version is available and notify users of its availability. If you disable or do not configure this policy setting, Internet Explorer will check for updates every 30 days (the default setting) and notify users if a new version is available. This policy setting is intended to help administrators maintain version control for Internet Explorer, because it prevents users from being notified when a new browser version is available.

The possible values for the Disable Periodic Check for Internet Explorer software updates setting are:

- Enabled
- Disabled
- Not Configured

Vulnerability

Although Microsoft thoroughly tests all patches and service packs before they are published, some organizations want to carefully control all of the software that is installed on their managed computers. You can enable the Disable Periodic Check for Internet Explorer software updates setting to ensure that computers will not automatically download and install updates for Internet Explorer.
Countermeasure
Configure the Disable Periodic Check for Internet Explorer software updates setting to Enabled.

Potential Impact
Internet Explorer will not be able to automatically download and install hotfixes and service packs. Therefore, administrators should have another process in place to automatically distribute software updates to all managed computers.

Disable software update shell notifications on program launch
This policy setting allows you to prevent user notification when programs that use the Microsoft Software Distribution Channel install new components. The Software Distribution Channel is a way to update software dynamically on user computers by using Open Software Distribution (OSD) technologies.

If you enable this policy setting, users will not be notified when their programs are updated through Software Distribution Channels. If you disable or do not configure this setting, users will be notified before their programs are updated. This policy setting is intended for administrators who want to use Software Distribution Channels to update their users’ programs without user intervention.

The possible values for the Disable software update shell notifications on program launch setting are:
- Enabled
- Disabled
- Not Configured

Vulnerability
Organizations that use OSD tools and technologies may prefer that their users not know when patches and service packs are installed on their computers, because users may attempt to stop an installation process before it completes.

Countermeasure
Configure the Disable software update shell notifications on program launch setting to Enabled.

Potential Impact
Users will not be notified when software updates are delivered through OSD technologies.
Make proxy settings per-machine (rather than per-user)

If you enable this policy setting, users will not be able to alter user-specific proxy settings. They must use the zones that are created for all users of the computers they access.

The possible values for the Make proxy settings per-machine (rather than per-user) setting are:

- Enabled
- Disabled
- Not Configured

Vulnerability

If you disable or do not configure this policy setting, users of the same computer will be able to establish their own proxy settings. This policy setting is intended to ensure that proxy settings remain uniformly in effect on the same computer and do not vary from user to user.

Countermeasure

Configure the Make proxy settings per-machine (rather than per-user) setting to Enabled.

Potential Impact

All users will be forced to use the proxy settings that are defined for the computer.

Security Zones: Do not allow users to add/delete sites

This policy setting allows you to disable the site management settings for security zones. (To see the site management settings for security zones, select Tools and then Internet Options from the menu bar in Internet Explorer. Click the Security tab, and then click Sites.) If you disable or do not configure this setting, users will be able to add or remove Web sites in the Trusted Sites and Restricted Sites zones. They will also be able to alter settings in the Local Intranet zone.

The possible values for the Security Zones: Do not allow users to add/delete sites setting are:

- Enabled
- Disabled
- Not Configured

Note: If you enable the Disable the Security page setting, which is located in

\User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel

the Security tab is removed from the interface. When it is enabled, this policy setting takes precedence over the Security Zones: Do not allow users to add/delete sites setting.

Vulnerability

If you do not configure this policy setting, users will be able to add or remove sites from the Trusted Sites and Restricted Sites zones at will and change settings in the Local Intranet zone. This configuration could allow sites that host malicious mobile code to be added to these zones, which users could execute.
**Countermeasure**

Configure the **Security Zones: Do not allow users to add/delete sites** setting to **Enabled**.

**Potential Impact**

Users will not be able to change site management settings for security zones that have been established by the administrator. When users need to add or remove sites from these Internet Explorer security zones, an administrator will have to configure them.

**Security Zones: Do not allow users to change policies**

This policy setting allows you to effectively disable the **Custom Level** button and Security level for the zone slider on the **Security** tab in the **Internet Options** dialog box. If you disable or do not configure this policy setting, users will be able to change the security zone settings. This policy setting can be used to prevent changes to the security zone policy settings that are established by the administrator.

The possible values for the **Security Zones: Do not allow users to change policies** setting are:
- **Enabled**
- **Disabled**
- **Not Configured**

**Note:** If you enable the **Disable the Security page** setting, which is located in

\User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel

the **Security** tab is removed from the interface. When it is enabled, this policy setting takes precedence over the **Security Zones: Do not allow users to change policies** setting.

**Vulnerability**

Users who change their Internet Explorer security settings could enable the execution of dangerous types of code from the Internet and Web sites that were listed in the **Restricted Sites** zone in the browser.

**Countermeasure**

Configure the **Security Zones: Do not allow users to change policies** setting to **Enabled**.

**Potential Impact**

Users will not be able to configure security settings for Internet Explorer zones.

**Security Zones: Use only machine settings**

This policy setting allows changes that the user makes to a security zone to apply to all users of that computer. If you disable or do not configure this policy setting, users of the same computer will be able to establish their own security zone settings. This policy setting is intended to ensure that security zone settings remain uniformly in effect on the same computer and do not vary from user to user.
The possible values for the Security Zones: Use only machine settings setting are:

- Enabled
- Disabled
- Not Configured

**Vulnerability**

Users who change their Internet Explorer security settings could enable the execution of dangerous types of code from the Internet and Web sites that were listed in the Restricted Sites zone in the browser.

**Countermeasure**

Configure the setting for Security Zones: Use only machine settings to Enabled.

**Potential Impact**

Users will not be able to configure security settings for Internet Explorer zones.

**Turn off Crash Detection**

This policy setting allows you to manage the crash detection feature of add-on management in Internet Explorer. If you enable this policy setting, a crash in Internet Explorer will be similar to one on a computer that runs Windows XP Professional with Service Pack 1 (SP1) and earlier: Windows Error Reporting will be invoked. If you disable this policy setting, the crash detection feature in add-on management will be functional.

The possible values for the Turn off Crash Detection setting are:

- Enabled
- Disabled
- Not Configured

**Vulnerability**

A crash report might contain sensitive information from the computer's memory.

**Countermeasure**

Configure the policy setting for Turn off Crash Detection setting to Enabled.

**Potential Impact**

Information about crashes that are caused by Internet Explorer add-ons will not be reported to Microsoft. If you experience frequent repeated crashes and need to report them to help troubleshoot the problem, the setting should temporarily be changed to Disabled.

**Do not allow users to enable or disable add-ons**

This policy setting allows you to manage whether users have the ability to allow or deny add-ons through Manage Add-ons. If you configure this policy setting to Enabled, users cannot enable or disable add-ons through Manage Add-ons. The only exception is if an add-on has been specifically entered into the Add-On List policy setting in a way that allows users to continue to manage the add-on through Manage Add-ons. If you
configure this policy setting to **Disabled**, the user will be able to enable or disable add-ons.

**Note:** For more information about how to manage Internet Explorer add-ons in Windows XP SP2, see KB article 883256, "How to manage Internet Explorer add-ons in Windows XP Service Pack 2" at http://support.microsoft.com/?kbid=883256.

The possible values for the **Do not allow users to enable or disable add-ons** setting are:

- Enabled
- Disabled
- Not Configured

**Vulnerability**

Users often choose to install add-ons that are not permitted by an organization's security policy. Such add-ons can pose a significant security and privacy risk to your network.

**Countermeasure**

Configure the value of the **Do not allow users to enable or disable add-ons** setting to **Enabled**.

**Potential Impact**

When the **Do not allow users to enable or disable add-ons** setting is enabled, users will not be able to enable or disable their own Internet Explorer add-ons. If your organization uses add-ons, this configuration may affect their ability to work.
Internet Explorer\Internet Control Panel\Security Page

You can configure the Internet Explorer Security Page Group Policy settings in the following location within the Group Policy Object Editor:

Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page

The individual policy settings for the Security Page are thoroughly documented in the Windows XP and Windows Server 2003 Help systems, and also on the Microsoft Web site. Therefore, this information is not repeated in this guide. You should consider the following general guidelines.

Vulnerability

If you allow users to configure their own security settings in Internet Explorer, they may increase their computers vulnerability to malicious software (malware). Also, users will be able to avoid any standard organizational security policies that are in place.

Countermeasure

Use the settings in the Internet Explorer\Internet Control Panel\Security Page node of Group Policy to configure appropriate values for security zones and security zone-related behavior.

Potential Impact

Windows XP SP2 and Windows Server 2003 SP1 introduce several new policy settings to help you secure Internet Explorer zone configuration across your environment. The default values for these policy settings provide enhanced security over earlier versions of Windows. However, you may need to customize these policy settings for your local environment. For example, you may want to add your business partners or suppliers to the Trusted Sites zone and not allow users to make their own changes to the zone lists.

Internet Explorer\Internet Control Panel\Advanced Page

The settings in this portion of the Administrative Template are equivalent to the settings that are available on the Advanced tab of the Internet Options dialog box in Internet Explorer.

The following two policy settings are available in both Windows Server 2003 with SP1 and Windows XP with SP2.

Allow software to run or install even if the signature is invalid

This policy setting allows you to manage whether downloaded software can be installed or run by users if the signature is invalid. An invalid signature might indicate that someone tampered with the file. If you enable this policy setting, users will be prompted to install or run files with an invalid signature. If you disable this policy setting, users cannot run or install files with an invalid signature.
The possible values for the **Allow software to run or install even if the signature is invalid** setting are:

- Enabled
- Disabled
- Not Configured

**Vulnerability**

Microsoft ActiveX® controls and file downloads often have digital signatures attached that certify the file's integrity and the identity of the signer (creator) of the software. Such signatures help ensure that unmodified software is downloaded and that you can positively identify the signer to determine whether you trust them enough to run their software. The validity of unsigned code cannot be ascertained.

**Countermeasure**

Configure the **Allow software to run or install even if the signature is invalid** setting to **Disabled** so that users cannot run unsigned ActiveX components.

**Potential Impact**

Some legitimate software and controls may have an invalid signature. You should carefully test such software in isolation before it is allowed to be used on your organization's network.

**Allow active content from CDs to run on user machines**

This policy setting allows you to determine whether active content on CDs can run on users' computers. Security-conscious organizations may wish to prevent the execution of ActiveX controls or other active content that is delivered on a CD.

The possible values for the **Allow active content from CDs to run on user machines** setting are:

- Enabled
- Disabled
- Not Configured

**Vulnerability**

Users may accidentally circumvent an organization's security policy if they run content that was delivered on a CD instead of over the network.

**Countermeasure**

You can configure the **Allow active content from CDs to run on user machines** setting to **Disabled**. This configuration will prevent the execution of active content that is stored on CDs.

**Potential Impact**

When this policy setting is enabled, applications that are designed to be installed from CD may not function properly without user intervention.
Allow third-party browser extensions

(This policy setting is only available in Windows Server 2003.)

Users may install third-party browser extensions, which are known as browser helper objects (BHOs). The Allow third-party browser extensions setting controls whether installed BHOs will load when Internet Explorer starts.

The possible values for the Allow third-party browser extensions setting are:

- Enabled
- Disabled
- Not Configured

Vulnerability

Third-party browser extensions are potentially dangerous, because they may contain vulnerabilities or even malicious code. Also, their installation may violate organizational security policies.

Countermeasure

Configure the Allow third-party browser extensions setting to Disabled.

Potential Impact

When you configure the Allow third-party browser extensions setting to Disabled, users will be able to install third-party browser extensions, but they will not be loaded when Internet Explorer starts. This configuration may impair user workflow or generate help desk calls.

Check for server certificate revocation

(This policy setting is only available in Windows Server 2003.)

When a Secure Sockets Layer (SSL) connection is established between the browser and a remote server, the server presents a certificate to the client computer to use in the initial security negotiation. When the Check for server certificate revocation setting is enabled, Internet Explorer will determine whether the presented certificate is on the issuing authority's certificate revocation list.

The possible values for the Check for server certificate revocation setting are:

- Enabled
- Disabled
- Not Configured

Vulnerability

Users may accidentally communicate with a server whose certificate has expired or been revoked by the issuing authority. Such an occurrence may lead to information disclosure or even active attacks if the remote server has been compromised.

Countermeasure

Configure the Check for server certificate revocation setting to Enabled.
Potential Impact
When the Check for server certificate revocation setting is enabled, users may receive warnings for sites they formerly believed to be trustworthy; it is necessary to educate them to help them make good trust decisions when they browse the Internet.

Check for signatures on downloaded programs
(This policy setting is only available in Windows Server 2003.)
Downloaded programs may be signed with Microsoft Authenticode® technology, which binds a digital signature to executable objects such as programs and ActiveX controls. When the Check for signatures on downloaded programs setting is enabled, Internet Explorer will check the digital signature of executable programs and display their identities before they are downloaded.
The possible values for the Check for signatures on downloaded programs setting are:
• Enabled
• Disabled
• Not Configured

Vulnerability
Users might download inappropriate or malicious content without realizing it.

Countermeasure
Configure the Check for signatures on downloaded programs setting to Enabled.

Potential Impact
When the Check for signatures on downloaded programs setting is enabled, users will see identity information for executable programs that have been signed.

Do not save encrypted pages to disk
(This policy setting is only available in Windows Server 2003.)
When Internet Explorer retrieves pages from a remote server, it stores the pages in its temporary file cache. This capability improves performance and provides the ability to go forward or backward in the browse history list without a reconnection to the host.
The possible values for the Do not save encrypted pages to disk setting are:
• Enabled
• Disabled
• Not Configured

Vulnerability
Cached pages from SSL-secured connections may contain sensitive information, like passwords or credit card numbers.

Countermeasure
Configure the Do not save encrypted pages to disk setting to Enabled.
Potential Impact

Pages that are retrieved over SSL connections will not be cached. This configuration may increase the use of network bandwidth as users’ browsers re-download pages that would have been cached if this policy setting were not in effect.

Empty Temporary Internet Files folder when browser is closed

(This policy setting is only available in Windows Server 2003.)

Pages that are retrieved by Internet Explorer are stored in its temporary file cache. Internet Explorer manages this cache according to the settings in the Temporary Internet Files Settings dialog box. After a file or object is downloaded, it remains in the cache until Internet Explorer removes it.

The possible values for the Empty Temporary Internet Files folder when browser is closed setting are:

- Enabled
- Disabled
- Not Configured

Vulnerability

Sensitive information may remain in the Temporary Internet Files folder after a user quits Internet Explorer and logs off. Another user on the same computer may be able to gain access to these files.

Countermeasure

Configure the Empty Temporary Internet Files folder when browser is closed setting to Enabled.

Potential Impact

Internet Explorer uses the Temporary Internet Files folder as a cache to improve browser performance. If you disable this feature you may increase the amount of time and bandwidth that users need to browse the Web.

Internet Explorer Security Features

The Computer Configuration Administrative Templates Windows Components Internet Explorer Security Features portion of the Windows Administrative Templates includes several policy settings that control various security features that were added to Internet Explorer 6.0 in Windows Server 2003 SP1 and Windows XP SP2. Each of these policy settings contains three subordinate settings:

- **Internet Explorer Processes.** This setting has three possible values: Enabled, Disabled, and Not Configured. When Enabled, the specified behavior is turned off for Internet Explorer and Windows Explorer processes. If you configure the setting to Disabled or Not Configured, the default behavior (described separately for each setting) remains in effect.

- **Process List.** This setting allows you to specify individual processes for which the security feature will be enabled or disabled. The process list controls which processes the feature control applies to; a setting value of 1 disables the feature for those processes, and a setting value of 0 enables the feature for those processes.
• **All Processes.** This setting has three possible values: **Enabled**, **Disabled**, and **Not Configured**. When **Enabled**, the specified behavior is turned off for Internet Explorer and Windows Explorer processes. If you configure the setting to **Disabled** or **Not Configured**, the default behavior (described separately for each setting) remains in effect.

**Binary Behavior Security Restriction**

Internet Explorer contains dynamic binary behaviors, which are components that encapsulate specific functionality for HTML elements to which they were attached. These binary behaviors are not controlled by any Internet Explorer security setting, which means they work on Web pages in the Restricted Sites zone.

In Windows XP SP2 and Windows Server 2003 SP1, there is a new Internet Explorer security setting for binary behaviors. This new security setting disables binary behaviors in the Restricted Sites zone by default, and provides a general mitigation to vulnerabilities in Internet Explorer binary behaviors.

In addition to the **Internet Explorer Processes**, **Process List**, and **All Processes** settings that were described earlier, the **Binary Behavior Security Restriction** setting allows you to permit individual behaviors with the **Admin-approved behaviors** setting. To control these binary and script behaviors, you can now set the appropriate zones to **Admin-approved** and then use this setting to specify the individual behaviors that can be run in each zone.

**Vulnerability**

Poorly written or malicious behaviors can be invoked by Web pages and cause instability or possible compromise.

**Countermeasure**

Disable the use of binary behaviors completely. Alternatively, you can specify a set of allowed behaviors with the **Admin-approved behaviors** setting.

**Potential Impact**

Applications that rely on binary behaviors may not function properly if you disable the behaviors on which they depend.

**MK Protocol Security Restriction**

This policy setting blocks the seldom-used MK protocol to reduce the attack surface area of a computer. Some older Web applications use the MK protocol to retrieve information from compressed files.

**Vulnerability**

Vulnerabilities may exist in the MK protocol handler, or in applications that call it.

**Countermeasure**

Because the MK protocol is not widely used, it should be blocked wherever it is not needed. Disable access to the MK protocol for all processes.

**Potential Impact**

Because resources that use the MK protocol will fail when you deploy this setting, you should ensure that none of your applications use the MK protocol.
Local Machine Zone Lockdown Security

When Internet Explorer opens a Web page, it places restrictions on what the page can do that are based on the Internet Explorer security zone to which the page belongs. There are several possible security zones, and each zone has different sets of restrictions. The security zone for a page is determined by its location. For example, pages that are located on the Internet will typically be in the more restrictive Internet security zone. They might not be allowed to perform some operations, such as access the local hard drive. Pages that are located on your organization's network would normally be in the Intranet security zone, and have fewer restrictions. The precise restrictions that are associated with most of these zones can be configured by the user through Internet Options on the Tools menu in Internet Explorer.

Before Windows XP SP2 and Windows Server 2003 SP1, the content on the local file system was treated as secure and was assigned to the Local Machine security zone (except for the content that is cached by Internet Explorer). This security zone typically allowed content to run in Internet Explorer with relatively few restrictions. With the release of these Service Packs, the default configuration of Internet Explorer now provides additional protection for the user because it locks down the Local Machine zone.

**Vulnerability**

Attackers often try to take advantage of the Local Machine zone to elevate privilege and compromise a computer. Many of the exploits that involve the Local Machine zone were mitigated by other changes to Internet Explorer in Windows XP SP2, and these changes were incorporated into Internet Explorer in Windows Server 2003 SP1. However, attackers may still be able to figure out ways to exploit the Local Machine zone.

**Countermeasure**

Configure the Local Machine Zone Lockdown Security setting to Enabled.

**Potential Impact**

Internet Explorer–based applications that use local HTML may not work properly if you configure the Local Machine Zone Lockdown Security setting to Enabled. Local HTML that is hosted in other applications will run under the less restrictive settings of the Local Machine zone that are used in previous version of Internet Explorer unless that application makes use of Local Machine Zone Lockdown.

**Consistent MIME Handling**

Internet Explorer uses Multipurpose Internet Mail Extensions (MIME) data to determine how to handle files that are downloaded from a Web server. The Consistent MIME Handling setting determines whether Internet Explorer requires that all file-type information that is provided by Web servers be consistent. For example, if the MIME type of a file is text/plain but the MIME data indicates that the file is really an executable file, Internet Explorer changes its extension to reflect this executable status. This capability helps ensure that executable code cannot masquerade as other types of data that may be trusted.

If you enable this policy setting, Internet Explorer examines all received files and enforces consistent MIME data for them. If you disable or do not configure this policy setting, Internet Explorer does not require consistent MIME data for all received files and will use the MIME data that is provided by the file.

**Note:** This setting works in conjunction with, but does not replace, the MIME Sniffing Safety Features settings.
Vulnerability
A malicious Web server could deliver executable content by using a non-executable MIME type, and a user who opened the content could be tricked and cause the content to execute.

Countermeasure
Configure the Consistent MIME Handling setting to Enabled.

Potential Impact
Applications that rely on the server to correctly set the MIME type of downloaded objects may fail when this setting is enabled if the server provides incorrect MIME type information.

MIME Sniffing Safety Features
MIME sniffing is a term for the process that examines the content of a MIME file to determine its context—whether it is a data file, an executable file, or some other type of file. This policy setting determines whether Internet Explorer MIME sniffing will prevent promotion of a file of one type to a more dangerous file type. When this policy setting is enabled, MIME sniffing will never promote a file of one type to a more dangerous file type. If you configure this policy setting to Disabled, Internet Explorer processes will allow a MIME sniff that promotes a file of one type to a more dangerous file type. For example, it is dangerous to promote a text file to an executable file because any code in the purported text file would be executed.

Vulnerability
A malicious Web site can provide content of one type with a MIME label that indicates it is safe.

Countermeasure
Configure the MIME Sniffing Safety Features setting for All Processes to Enabled.

Potential Impact
Applications that rely on mislabeled MIME types for correct function will break when this policy setting is enabled.

Object Caching Protection
In previous versions of Internet Explorer, a Web page could reference an object that is cached from another Web site. The Object Caching Protection setting allows you to prevent such references to cached objects.

Vulnerability
A malicious server could download an object to a user's computer and then activate it through code on another site, perhaps in a different Internet Explorer zone. For example, an attacker could use this method to create scripts that listen to events or content in another frame, such as credit card numbers or other sensitive data that is typed in the other frame.
Countermeasure

Configure the Object Caching Protection for Internet Explorer Processes to Enabled.

Potential Impact

Properly written applications should not rely on cross-domain object access. Those applications that do will not work when this policy setting is enabled.

Scripted Window Security Restrictions

Internet Explorer allows scripts to programmatically open, resize, and reposition various types of windows. The Scripted Window Security Restrictions setting restricts pop-up windows and prohibits the display of windows in which the title and status bars are not visible to the user or that hide other windows’ title and status bars. If you enable this policy setting, Windows will apply these restrictions for Windows Explorer and Internet Explorer processes. If you disable or do not configure this policy setting, scripts can continue to create pop-up windows and windows that hide other windows.

Note that there are many third-party tools that attempt to control Internet Explorer pop-up windows. Many of those tools restrict pop-up windows in a similar way to this setting. Third-party pop-up blockers do not usually interfere with this setting, and this setting should have no effect on those blockers.

Vulnerability

Disreputable Web sites will resize windows to either hide other windows or force users to interact with a window that contains malicious code.

Countermeasure

Configure the Scripted Window Security Restrictions setting for Internet Explorer Processes to Enabled.

Potential Impact

Web applications that need to resize or position windows may not work correctly when this setting is in effect.

Protection From Zone Elevation

Internet Explorer places restrictions on each Web page it opens that depend on the location of the Web page (such as Internet zone, Intranet zone, or Local Machine zone). Web pages on a local computer have the fewest security restrictions and reside in the Local Machine zone, which makes the Local Machine security zone a prime target for malicious attackers.

If you enable the Internet Explorer Processes – Protection from Zone Elevation setting, any zone can be protected from zone elevation by Internet Explorer processes. This approach stops content that runs in one zone from gaining the elevated privileges of another zone.

Vulnerability

Malicious Web pages may attempt to elevate themselves from their current zone into another zone with higher privileges.
Countermeasure
Configure the Protection from Zone Elevation setting for Internet Explorer Processes to Enabled.

Potential Impact
None.

Restrict ActiveX Install
This setting allows you to block ActiveX control installation prompts for Internet Explorer processes. If you enable this policy setting, users will not be prompted when a page includes an ActiveX control that has to be manually installed; they will not be able to install the control from the Web page. If you disable this policy setting, ActiveX control installation prompts will not be blocked.

Vulnerability
Users often choose to install software such as ActiveX controls that are not permitted by their organization’s security policy. Such software can pose significant security and privacy risks to networks.

Countermeasure
Configure the Restrict ActiveX Install setting for Internet Explorer Processes to Enabled.

Potential Impact
If you enable this policy setting, users will not be able to install authorized legitimate ActiveX controls, such as those that are used by Windows Update. If you enable this policy setting, ensure that you implement some alternative way to deploy security updates such as Windows Server Update Services (WSUS). For more information about WSUS, see the Windows Server Update Services Product Overview page at www.microsoft.com/windowsserversystem/updateservices/evaluation/overview.mspx.

Restrict File Download
When the Restrict File Download setting is enabled, file download prompts that are not user-initiated are blocked for Internet Explorer processes.

Vulnerability
In certain circumstances, Web sites can initiate file download prompts without interaction from users. This technique can allow Web sites to put unauthorized files on users’ computers if they click the wrong button and accept the download.

Countermeasure
Configure the Restrict File Download value for Internet Explorer Processes to Enabled.

Potential Impact
None. There is no legitimate reason for a Web site to start transferring a file to a user’s workstation without a user request to do so.
Add-on Management
This policy setting, along with the Add-on List setting, allows you to control Internet Explorer add-ons. By default, the Add-on List setting defines a list of add-ons to be allowed or denied through Group Policy. The Deny all add-ons unless specifically allowed in the Add-on List setting ensures that all add-ons are assumed to be denied unless they are specifically listed in the Add-on List setting.

If you enable this policy setting, Internet Explorer only allows add-ins that are specifically listed (and allowed) through the Add-on List. If you disable this setting, users may use Add-on Manager to allow or deny any add-ons.

You should consider using both the Deny all add-ons unless specifically allowed in the Add-on List and the Add-on List settings to control the add-ons that can be used in your environment. This approach will help ensure that only authorized add-ons are used.

Vulnerability
Poorly written or malicious add-ons may destabilize or compromise user computers.

Countermeasure
Configure the Add-on List setting to the list of trusted Internet Explorer add-ons to which your users should have access. Then configure the Deny all add-ons unless specifically allowed in the Add-on List to Enabled.

Potential Impact
If you configure the Deny all add-ons unless specifically allowed in the Add-on List setting to Enabled, users will not be able to install or configure their own add-ons.

Network Protocol Lockdown
Windows Server 2003 SP1 and Windows XP SP2 add the capability for administrators to prevent the execution of active content that is downloaded through specific network protocols. Administrators can specify individual protocols (including HTTP and HTTPS) in the Network Protocol Lockdown setting to control which protocols may be used to obtain active content.

Vulnerability
Users may download and execute malicious content from untrusted sources.

Countermeasure
Use the Restricted Protocols Per Security Zone setting to define which protocols may be used to download content in each zone. Then configure the Network Protocol Lockdown setting for Internet Explorer Processes to Enabled.

Potential Impact
Users may not be able to run applications or use pages that include active content if the per-zone controls are set. You must thoroughly test applications in each zone to ensure that they work properly when protocol lockdown is used.
**Internet Information Services**

Microsoft Internet Information Services (IIS) 6.0, the Windows Server 2003 built-in Web server, makes it easy to share documents and information across a company intranet and the Internet. You can configure the IIS setting in the following location within the Group Policy Object Editor:

```
Computer Configuration\Administrative Templates\Windows Components\Internet Information Services
```

**Prevent IIS installation**

IIS 6.0 is not installed by default in Windows Server 2003. You can enable the **Prevent IIS installation** setting to prevent the installation of IIS to install on computers in your environment.

The possible values for the **Prevent IIS installation** setting are:

- Enabled
- Disabled
- Not Configured

**Vulnerability**

Previous versions of IIS and applications that relied on it for network access had some serious security vulnerabilities that could be exploited remotely. Although IIS 6.0 is much more secure than its predecessors, it is possible that there are new vulnerabilities that have yet to be discovered and publicized. Therefore, organizations may want to ensure that IIS cannot be installed on computers other than those that are specified as Web servers.

**Countermeasure**

Configure the **Prevent IIS installation** setting to **Enabled**.

**Potential Impact**

You will not be able to install Windows components or applications that require IIS. Users who install Windows components or applications that require IIS may not see an error message or warning that IIS cannot be installed because of this Group Policy setting. This policy setting will have no effect if it is enabled on a computer on which IIS is already installed.
Terminal Services

The Terminal Services component of Windows Server 2003 builds on the solid foundation that was provided by the application server mode in Windows 2000 Terminal Services, and now includes the new client and protocol capabilities in Windows XP. Terminal Services allow you to deliver Windows-based applications, or the Windows desktop itself, to almost any computing device—including those that cannot run Windows.

Terminal Services in Windows Server 2003 can enhance an organization’s software deployment capabilities for a variety of scenarios, because it allows substantial flexibility in application and management infrastructure. When a user runs an application on Terminal Server, the application execution takes place on the server, and only keyboard, mouse and display information is transmitted over the network. Each user sees only his or her individual session, which is managed transparently by the server operating system, and each session is independent of any other client session.

You can configure the Terminal Server Group Policy settings in the following location within the Group Policy Object Editor:

```
Computer Configuration\Administrative Templates\Windows Components\Terminal Services
```

**Deny log off of an administrator logged in to the console session**

This policy setting specifies whether an administrator who attempts to connect to the console of a server can log off an administrator who is currently logged on to the console. The console session is also known as Session 0. Console access can be obtained by using the /console switch from Remote Desktop Connection in the computer field name or from the command line.

The possible values for the Deny log off of an administrator logged in to the console session setting are:

- Enabled
- Disabled
- Not Configured

If you enable the Deny log off of an administrator logged in to the console session setting, no one will be able to log off an administrator who is connected to the computer. If you disable this policy setting, one administrator will be allowed to log off another administrator. If you do not configure this policy setting, one administrator can log off another administrator, but this permission can be revoked at the local computer policy level.

This policy is useful when the currently connected administrator does not want to be logged off by another administrator. If a connected administrator is logged off, they will lose any unsaved data.

**Vulnerability**

An attacker who has managed to establish a Terminal Server session and acquired administrative privileges could make it even more difficult to regain control of the computer if they forcibly log off an administrator who attempts to log on to the server at the Session 0 console. The value of this countermeasure is diminished by the fact that an
attacker who has gained sufficient privileges to log off other users has almost complete control of the computer already.

**Countermeasure**

Configure the **Deny log off of an administrator logged in to the console session** setting to **Enabled**.

**Potential Impact**

An administrator will not be able to forcibly log off other administrators from the Session 0 console.

**Do not allow local administrators to customize permissions**

This policy setting allows you to control administrators’ rights to customize security permissions in the Terminal Services Configuration (TSCC) tool. If you enable this policy setting, administrators will not be able to make changes to the security descriptors for user groups in the TSCC **Permissions** tab. In the default configuration, administrators are able to make such changes.

If you enable the **Do not allow local administrators to customize permissions** setting, the TSCC **Permissions** tab cannot be used to customize per-connection security descriptors or to change the default security descriptors for an existing group. All of the security descriptors become Read Only. If you disable or do not configure this policy setting, server administrators have full Read/Write privileges to the user security descriptors in the TSCC **Permissions** tab.

The possible values for the **Do not allow local administrators to customize permissions** setting are:

- Enabled
- Disabled
- Not Configured

**Note:** The preferred way to manage user access is to add users to the Remote Desktop Users group.

**Vulnerability**

An attacker who gains administrative permissions on a server that runs Terminal Services can modify permissions by using the TSCC tool to prevent other user connections to the server and create a DoS condition.

The value of this countermeasure is diminished by the fact that an attacker who has gained administrative privileges has already taken over complete control of the computer.

**Countermeasure**

Configure the **Do not allow local administrators to customize permissions** setting to **Enabled**.

**Potential Impact**

The TSCC **Permissions** tab cannot be used to customize per-connection security descriptors or to change the default security descriptors for an existing group.
**Sets rules for remote control of Terminal Services user sessions**

This policy setting specifies the level of remote control that is permitted in a Terminal Server session. Remote control can be established with or without the session user's permission. You can use this policy setting to select one of two levels of remote control: **View Session** permits the remote control user to watch a session, and **Full Control** permits the remote control user to interact with the session. If you enable the **Sets rules for remote control of Terminal Services user sessions** setting, administrators can remotely interact with a user's Terminal Server session in accordance with the specified rules. To set these rules, select the desired level of control and permission in the Options list. To disable remote control, select **No remote control allowed**. If you disable or do not configure this policy setting, the server administrator can determine the remote control rules by using the TSCC tool. By default, remote control users can have full control with the session user's permission.

The possible values for the **Sets rules for remote control of Terminal Services user sessions** setting are:

- Enabled with options for:
  - No remote control allowed
  - Full Control with user's permission
  - Full Control without user's permission
  - View Session with user's permission
  - View Session without user's permission
- Disabled
- Not Configured

**Note:** This setting exists in both the Computer Configuration and User Configuration nodes. When it is configured in both places, the Computer Configuration setting takes precedence over the same setting in User Configuration.

**Vulnerability**

An attacker who gains administrative privileges on the server could use the remote control feature of Terminal Services to observe the actions of other users. Such a situation could result in the disclosure of confidential information. The value of this countermeasure is diminished by the fact that an attacker who gains administrative privileges has already established complete control of the computer.

**Countermeasure**

Configure the **Sets rules for remote control of Terminal Services user sessions** setting to **Enabled** and select the **No remote control allowed** option.

**Potential Impact**

Administrators will not be able to use the remote control feature to assist other Terminal Services users.
**Client/Server Data Redirection**

Terminal Services allows data and resources from the client and server to be redirected. For example, data that is printed from a server application can be redirected to the client, or the client clipboard can be used in server applications. The settings in the "Client/Server data redirection" section of Group Policy allow you to customize which types of redirection are permitted.

The Terminal Server Data Redirection settings can be configured in the following location within the Group Policy Object Editor:

```
Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Client\Server data redirection
```

**Allow Time Zone Redirection**

This policy setting specifies whether to allow the client computer to redirect its time zone settings to the Terminal Server session. By default, the session time zone is the same as the server time zone, and the client computer cannot redirect its time zone information.

If you enable the **Allow Time Zone Redirection** setting, clients that are capable of time zone redirection can send their time zone information to the server. The server base time is then used to calculate the current session time. Current session time is the server base time plus the client time zone. Currently, Remote Desktop Connection and Windows CE 5.1 are the only clients that are capable of time zone redirection. Session 0, the console session, always has the server time zone and settings. To change the computer's time and time zone, connect to Session 0.

If you disable the **Allow Time Zone Redirection** setting, time zone redirection cannot occur. If you do not configure this policy setting, time zone redirection is not specified at the Group Policy level, and the default configuration is for time zone redirection to be turned off. When an administrator changes this policy setting, only new connections display the behavior that is specified by the new setting. Sessions that were initiated before the change must log off and reconnect to be affected by the new setting. Microsoft recommends that all users log off the server after this policy setting is changed.

The possible values for the **Allow Time Zone Redirection** setting are:

- Enabled
- Disabled
- Not Configured

*Note:* Time zone redirection is only possible for connections to a Windows Server family Terminal Server.

**Vulnerability**

Time zone data could be forwarded from the user's Terminal Server session to the user's local computer without any direct user interaction.

**Countermeasure**

Configure the **Allow Time Zone Redirection** setting to **Disabled**.

**Potential Impact**

Time zone redirection will not be possible.
Do not allow clipboard redirection

This policy setting controls whether clipboard contents can be shared (clipboard redirection) between a remote computer and a client computer in a Terminal Server session. You can use this setting to prevent the redirection of clipboard data between the remote computer and the local computer. By default, Terminal Services allows this clipboard redirection.

If you enable the **Do not allow clipboard redirection** setting, users cannot redirect clipboard data. If you disable this policy setting, Terminal Services will always allow clipboard redirection. If you do not configure this policy setting, clipboard redirection is not specified at the Group Policy level. However, an administrator can still disable clipboard redirection by using the TSCC tool.

The possible values for the **Do not allow clipboard redirection** setting are:

- Enabled
- Disabled
- Not Configured

**Vulnerability**

Data could be forwarded from a user's terminal server session to the user's local computer without any direct user interaction.

**Countermeasure**

Configure the **Do not allow clipboard redirection** setting to **Enabled**.

**Potential Impact**

Clipboard redirection will not be possible.

Allow audio redirection

This policy setting specifies whether users can choose where to play the remote computer's audio output during a Terminal Server session. Users can click the **Remote computer sound** option button on the **Local Resources** tab of Remote Desktop Connection to choose whether to play audio on the remote computer or the local computer. Users can also choose to disable the audio. By default, users cannot apply audio redirection when they connect through Terminal Services to a server that runs Windows Server 2003. Users who connect to a computer that runs Windows XP Professional can apply audio redirection by default.

If you enable the **Allow audio redirection** setting, users can apply audio redirection. If you disable this policy setting, users cannot apply audio redirection. If you do not configure this policy setting, audio redirection is not specified at the Group Policy level. However, an administrator can still enable or disable audio redirection by using the TSCC tool.

The possible values for the **Allow audio redirection** setting are:

- Enabled
- Disabled
- Not Configured
**Vulnerability**
Data could be forwarded from the user's Terminal Server session to the user's local computer without any direct user interaction.

**Countermeasure**
Configure the **Allow audio redirection** setting to **Disabled**.

**Potential Impact**
Audio redirection will not be possible.

**Do not allow COM port redirection**
This policy setting can be used to prevent the redirection of data to client communication ports from the remote computer in a Terminal Server session. If you enable this policy setting, users cannot redirect data to COM port peripherals or map local COM ports while they are logged on to a Terminal Server session. By default, Terminal Services allows COM port redirection.

If you enable the **Do not allow COM port redirection** setting, users will not be able to redirect server data to the local COM port. If you disable this policy setting, Terminal Services COM port redirection is always allowed. If you do not configure this policy setting, COM port redirection is not specified at the Group Policy level. However, an administrator can still disable COM port redirection by using the TSCC tool.

The possible values for the **Do not allow COM port redirection** setting are:
- Enabled
- Disabled
- Not Configured

**Vulnerability**
Data could be forwarded from the user's Terminal Server session to the user's local computer without any direct user interaction.

**Countermeasure**
Configure the **Do not allow COM port redirection** setting to **Enabled**.

**Potential Impact**
COM port redirection will not be possible.

**Do not allow client printer redirection**
This policy setting specifies whether client printers can be mapped in Terminal Server sessions. You can use this policy setting to prevent print job redirection to users’ local (client) computers from the remote computer. By default, Terminal Services allows client printers to be mapped.

If you enable the **Do not allow client printer redirection** setting, users cannot redirect print jobs from the remote computer to a local client printer in Terminal Server sessions. If you disable this policy setting, users can redirect print jobs with client printer mapping. If you do not configure this policy setting, client printer mapping is not specified at the Group Policy level. However, an administrator can still disable client printer mapping by using the TSCC tool.
The possible values for the Do not allow client printer redirection setting are:
- Enabled
- Disabled
- Not Configured

**Vulnerability**
Data could be forwarded from the user's Terminal Server session to the user's local computer without any direct user interaction.

**Countermeasure**
Configure the Do not allow client printer redirection setting to Enabled.

**Potential Impact**
Printer redirection will not be possible.

**Do not allow LPT port redirection**
This policy setting specifies whether to prevent the redirection of data to client parallel ports (LPT) during a Terminal Server session. You can use this setting to prevent users from mapping local LPT ports to redirect data from the remote computer to local LPT port peripherals. By default, Terminal Services allows LPT port redirection.

If you enable the Do not allow LPT port redirection setting, users in a Terminal Server session cannot redirect server data to their local LPT port. If you disable this policy setting, LPT port redirection is always allowed. If you do not configure this setting, LPT port redirection is not specified at the Group Policy level. However, an administrator can still disable local LPT port redirection by using the TSCC tool.

The possible values for the Do not allow LPT port redirection setting are:
- Enabled
- Disabled
- Not Configured

**Vulnerability**
Data could be forwarded from the user's Terminal Server session to the user's local computer without any direct user interaction.

**Countermeasure**
Configure the Do not allow LPT port redirection setting to Enabled.

**Potential Impact**
LPT port redirection will not be possible.

**Do not allow drive redirection**
By default, Terminal Services maps client drives automatically upon connection. Mapped drives appear in the session folder tree in Windows Explorer or My Computer in the format <drive_letter> on <computer_name>. You can use the Do not allow drive redirection setting to override this behavior.
You can enable the **Do not allow drive redirection** setting to prevent client drive redirection in Terminal Server sessions. If you disable this policy setting, client drive redirection is always allowed. If you do not configure this policy setting, client drive redirection is not specified at the Group Policy level. However, an administrator can still disable client drive redirection by using the TSCC tool.

The possible values for the **Do not allow drive redirection** setting are:

- Enabled
- Disabled
- Not Configured

**Vulnerability**

Data could be forwarded from the user's Terminal Server session to the user's local computer without any direct user interaction.

**Countermeasure**

Configure the **Do not allow drive redirection** setting to **Enabled**.

**Potential Impact**

Drive redirection will not be possible.

**Do not set default client printer to be default printer in a session**

This policy setting directs Terminal Services to not specify the default client printer as the default printer for Terminal Server sessions. By default, Terminal Services automatically designates the default client printer as the default printer. This setting can override the default configuration.

If you enable the **Do not set default client printer to be default printer in a session** setting, the Terminal Server cannot set the default client printer as the default printer for the session. Instead, the server specifies the default at the server. If you disable this policy setting, the default printer is always the default client printer. If you do not configure this setting, the default printer designation is not enforced at the Group Policy level. However, an administrator can configure the default printer for client sessions by using the TSCC tool.

The possible values for the **Do not set default client printer to be default printer in a session** setting are:

- Enabled
- Disabled
- Not Configured

**Vulnerability**

Data could be forwarded from the user's Terminal Server session to the user's local computer without any direct user interaction.

**Countermeasure**

Configure this policy setting to **Enabled**.
Potential Impact
A client computer’s default printer will not be the default printer during its Terminal Server session.

Encryption and Security
You can configure the Terminal Server Encryption and Security settings in the following location within the Group Policy Object Editor:

Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Encryption and Security

Set Client Connection Encryption Level
This policy setting specifies whether to enforce an encryption level for all data that is sent between the client and the remote computer during a Terminal Server session.

If you enable the Set Client Connection Encryption Level setting you can specify the level of encryption for all connections to the server. By default, encryption is set to High Level. If you disable or do not configure this policy setting, no encryption level is enforced through Group Policy. However, administrators can set the encryption level on the server by using the TSCC tool.

The possible values for the Set Client Connection Encryption Level setting are:

- **Enabled** with encryption options for:
  - **Client Compatible.** This value encrypts the data that is sent between the client and server at the maximum key strength that is supported by the client. Use this level when the remote computer runs in an environment that contains mixed or legacy clients.
  - **High Level.** This value encrypts the data that is sent between the client and server with strong 128-bit encryption. Use this level when the remote computer runs in an environment that contains 128-bit clients only, such as Remote Desktop Connection clients. Clients that do not support this level of encryption cannot connect.
  - **Low Level.** This value encrypts the data that is sent from the client to the server with 56-bit encryption. When you specify Low Level, data that is sent from the server to the client is not encrypted.

- **Disabled**

- **Not Configured**

**Important:** If FIPS compliance has already been enabled by the System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing setting, you cannot change the encryption level through this policy setting or with the TSCC tool.

Vulnerability
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.

Countermeasure
Configure the Set Client Connection Encryption Level setting to High Level.
Potential Impact

Clients that do not support 128-bit encryption will be unable to establish Terminal Server sessions.

Always prompt client for a password on connection

This policy setting specifies whether Terminal Services always prompts the client 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 entered a password in the Remote Desktop Connection client.

If you enable the Always prompt client for a password on connection setting, users will not be able to automatically log on to Terminal Services, even if they supplied their passwords in the Remote Desktop Connection client. They will be prompted for a password to log on. If you disable this policy setting, users can always log on automatically to Terminal Services automatically if they supply their passwords in the Remote Desktop Connection client. If you do not configure this policy setting, automatic logon is not specified at the Group Policy level. However, an administrator can still enforce password prompting by using the TSCC tool.

The possible values for the Always prompt client for a password on connection setting are:

• Enabled
• Disabled
• Not Configured

Vulnerability

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.

Countermeasure

Configure the Always prompt client for a password on connection setting to Enabled.

Potential Impact

Users will always have to enter their password when they establish new Terminal Server sessions.
**RPC Security Policy**

You can configure the Terminal Server RPC Security setting in the following location within the Group Policy Object Editor:

```
Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Encryption and Security\RPC Security Policy
```

**Secure Server (Require Security)**

This policy setting specifies whether a Terminal Server requires secure remote procedure call (RPC) communication with all clients or allows unsecured communication. You can use this setting to strengthen the security of RPC communication with clients if you allow only authenticated and encrypted requests.

If you enable the **Secure Server (Require Security)** setting, the Terminal Server will only accept requests from RPC clients that support secure requests. It will not allow unsecured communication with clients that are not trusted. If you disable this policy setting, the Terminal Server will always accept requests at any level of security for all RPC traffic. However, unsecured communication is allowed for RPC clients that do not respond to the request. If you do not configure this policy setting, unsecured communication will be allowed.

The possible values for the **Secure Server (Require Security)** setting are:

- Enabled
- Disabled
- Not Configured

**Note:** Use the RPC interface to administer and configure Terminal Services.

**Vulnerability**

Unsecure RPC communication exposes the server to man-in-the-middle attacks and data disclosure attacks. A man-in-the-middle attack occurs when an intruder captures packets between a client and server, modifies them, and then allows the packets to be exchanged. Usually the attacker will modify the information in the packets in an attempt to cause either the client or server to reveal sensitive information.

**Countermeasure**

Configure the **Secure Server (Require Security)** setting to **Enabled**.

**Potential Impact**

Clients that do not support secure RPC will be unable to remotely manage the server.
Sessions

You can configure additional Terminal Server RPC Security settings in the following location within the Group Policy Object Editor:

```
Computer Configuration\Administrative Templates\Windows Components\Terminal Services Encryption and Security\Sessions
```

Set time limit for disconnected sessions

This policy setting specifies a time limit for disconnected Terminal Server sessions. You can use this setting to specify the maximum amount of time that a disconnected session remains active on the server. By default, Terminal Services allows users to disconnect from a remote session but does not require them to log off and end the session. When a session is in a disconnected state, programs may continue to run even though the user is no longer actively connected. By default, these disconnected sessions are maintained for an unlimited time on the server.

You can enable the **Set time limit for disconnected sessions** setting to delete disconnected sessions from the server after a specified amount of time. To enforce the default behavior that sustains disconnected sessions for an unlimited time, select **Never**. If you disable or do not configure this policy setting, no time limit is specified for disconnected sessions at the Group Policy level.

The possible values for the **Set time limit for disconnected sessions** setting are:

- Enabled with time specification options for:
  - Never
  - 1 minute
  - 5 minutes
  - 10 minutes
  - 15 minutes
  - 30 minutes
  - 1 hour
  - 2 hours
  - 3 hours
  - 1 day
  - 2 days
- Disabled
- Not Configured

**Note:** This policy setting does not apply to console sessions such as Remote Desktop sessions with computers that run Windows XP Professional. This policy setting exists in both the Computer Configuration and User Configuration nodes. When it is configured in both places, the Computer Configuration setting takes precedence over the same setting in the User Configuration node.

Vulnerability

Each Terminal Server session uses system resources. Unless sessions that have been disconnected for an extended period of time are forcibly terminated, your servers may run low on resources.
**Countermeasure**

Configure the **Set time limit for disconnected sessions** setting to **Enabled** and select **1 day** as the option in the **End a disconnected session** list box.

**Potential Impact**

Users who forget to log off of Terminal Server sessions will have those sessions forcibly terminated after 24 hours of inactivity.

**Allow reconnection from original client only**

This policy setting allows you to prevent Terminal Services reconnections to disconnected sessions by users who use different computers than the original client computer from which they created the session. By default, Terminal Services allows users to reconnect to disconnected sessions from any client computer.

If you enable the **Allow reconnection from original client only** setting, users will be able to reconnect to disconnected sessions only from the original client computer. If a user attempts to connect to the disconnected session from another computer, a new session is created instead. If you disable this setting, users can always connect to a disconnected session from any computer. If you do not configure this setting, no session reconnection rules are specified at the Group Policy level.

The possible values for the **Allow reconnection from original client only** setting are:

- Enabled
- Disabled
- Not Configured

**Important:** This setting is only supported for Citrix ICA clients that provide a serial number when they connect; the setting is ignored if the user connects with a Windows client. This setting exists in both the Computer Configuration and User Configuration nodes. When it is configured in both places, the Computer Configuration setting takes precedence over the same setting in the User Configuration node.

**Vulnerability**

By default, users can re-establish disconnected Terminal Server sessions from any computer. If you enable this setting, you ensure that users can only reconnect from the computer that was originally used to establish the connection. The value of this countermeasure is diminished by the fact that it is only enforced by users who connect with Citrix ICA clients.

**Countermeasure**

Configure the **Allow reconnection from original client only** setting to **Enabled**.

**Potential Impact**

Users who connect with Citrix ICA clients will only be able to re-establish disconnected sessions with the computer that they used to establish the session.
Windows Explorer

You can configure the following Windows Explorer setting in the following location within the Group Policy Object Editor:

Computer Configuration\Administrative Templates\Windows Components\Windows Explorer

Turn off shell protocol protected mode

This policy setting allows you to configure the amount of functionality for the shell protocol. Full functionality of this protocol allows applications to open folders and launch files. The protected mode reduces functionality and only allows applications to open a limited set of folders. Applications are not able to open files when this protocol is in its protected mode.

Microsoft recommends that you leave this protocol in the protected mode to increase the security of Windows. If you enable the Turn off shell protocol protected mode setting, the protocol allows any application to open any folders or files. If you disable or do not configure this policy setting, the protocol is in protected mode and applications can only open a limited set of folders.

The possible values for the Turn off shell protocol protected mode setting are:
• Enabled
• Disabled
• Not Configured

Vulnerability

Full shell protocol functionality allows applications to open files and folders. This capability can result in accidental invocation of malicious or destructive software and unauthorized information disclosure. It could also result in a denial of service condition.

Countermeasure

Configure the Turn off shell protocol protected mode setting to Enabled.

Potential Impact

If you enable the Turn off shell protocol protected mode setting, Web pages that depend on use of the shell protocol will not function properly.

Windows Messenger

Windows Messenger is used to send instant messages to other users on a computer network. The messages may include files and other attachments.

You can configure the prescribed Windows Messenger setting in the following location within the Group Policy Object Editor:

Computer Configuration\Administrative Templates\Windows Components\Windows Messenger
Do not allow Windows Messenger to be run

The Do not allow Windows Messenger to be run setting allows you to disable Windows Messenger. You can configure this setting to Enabled to prevent the use of Windows Messenger.

Note: If you configure this setting to Enabled, Remote Assistance cannot use Windows Messenger and users cannot use MSN® Messenger.
**Windows Update**

Windows Update is used to download items such as security fixes, critical updates, the latest Help files, drivers, and Internet products. You can configure the Windows Update settings in the following location within the Group Policy Object Editor:

```
Computer Configuration\Administrative Templates\Windows Components\Configure Automatic Updates
```

**Configure Automatic Updates**

This policy setting specifies whether computers in your environment will receive security updates and other important downloads through the Windows automatic update service.

If you enable the Configure Automatic Updates setting, Windows determines when the computers are online and uses their Internet connection to search the Windows Update Web site for updates that apply to them. If you disable this policy setting, updates must be manually downloaded and installed from the Windows Update Web site at http://windowsupdate.microsoft.com. If you do not configure this setting, no use of Automatic Updates is specified at the Group Policy level. However, an administrator can still configure Automatic Updates through the Control Panel.

The possible values for the Configure Automatic Updates setting are:

- **Enabled**, with options in the Configure automatic updating list box for:
  - **2. Notify before downloading any updates and notify again before installing them.**
    
    When Windows finds updates that apply to computers in your environment, an icon appears in the status area with a message that updates are ready to download. When you click the icon or message you can select specific updates. Windows then downloads the selected updates in the background. When the download is complete, the icon appears in the status area again, with notification that the updates are ready to install. When you click the icon or message, you can select which updates to install.

  - **3. Download the updates automatically and notify when they are ready to be installed.**

    This value is the default configuration. Windows finds updates that apply to computers in your environment and downloads them in the background; the user is not notified or interrupted during this process. When the download is complete, an icon appears in the status area with notification that the updates are ready to install. You can click the icon or message select which updates to install.

  - **4. Automatically download updates and install them on the schedule specified below.**

    Specify the schedule using the options in the Group Policy setting. If no schedule is specified, the default schedule for all installations will be everyday at 3:00 A.M. If any updates require a restart to complete the installation, Windows will restart the affected computers automatically. If a user is logged on to a computer when Windows is ready to restart, the user will be notified and given the option to delay the restart.

- **Disabled**

- **Not Configured**
To enable this setting, click Enabled, and then select one of the options (2, 3, or 4). If you select 4, you can set a recurring schedule. If you don’t specify a schedule, installations will occur daily at 3:00 A.M.

**Vulnerability**

Although Windows Server 2003 and Windows XP were 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.

**Countermeasure**

Configure the **Configure Automatic Updates** setting to Enabled and select 4. **Automatically download updates and install them on the schedule specified below** from the **Configure automatic updating** list box.

**Potential Impact**

Critical operating system updates and service packs will automatically download and install at 3:00 A.M. daily.

**No auto-restart for scheduled Automatic Updates installations**

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.

**Vulnerability**

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.
**Countermeasure**

Configure the **No auto-restart for scheduled Automatic Updates installations** setting to **Disabled**.

**Potential 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.

**Reschedule Automatic Updates scheduled installations**

This policy setting specifies the amount of time for Automatic Updates to wait (after startup) before it proceeds with a scheduled installation that was previously missed. If you enable this setting, the installation that did not take place earlier will commence a specified number of minutes after the computer is next started. If you disable or do not configure this setting, scheduled installations that were missed previously will occur with the next scheduled installation.

The possible values for the **Reschedule Automatic Updates scheduled installations** setting are:

- Enabled, with the option to specify a time between 1 to 60 minutes.
- 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.

**Vulnerability**

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.

**Countermeasure**

Configure the **Reschedule Automatic Updates scheduled installations** setting to **Enabled** and specify 10 minutes.

**Potential impact**

Automatic Updates will not start until 10 minutes after the computer restarts.

**Specify intranet Microsoft update service location**

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).

The possible values for the **Specify intranet Microsoft update service location** setting are:

- **Enabled.** After you select this value, specify the intranet update server’s name and the statistics server’s name in the **Properties** dialog box.
- **Disabled**
- **Not Configured**

**Note:** If you configure the **Configure Automatic Updates** setting to **Disabled**, this policy setting has no effect.

**Vulnerability**

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.

**Countermeasure**

Configure the **Specify intranet Microsoft update service location** setting to **Enabled**. Then specify the intranet update server’s name and the statistics server’s name in the **Properties** dialog box.

**Potential Impact**

Critical updates and service packs will have to be proactively managed by the organization’s IT staff.

**System**

You can configure the prescribed System computer setting in the following location within the Group Policy Object Editor:

```
Computer Configuration\Administrative Templates\System
```

**Turn off Autoplay**

Autoplay starts reading from a drive as soon as you insert media in the drive, which causing the setup file for programs or audio media to start immediately. You can enable the **Turn off Autoplay** setting to prevent Autoplay functionality. Autoplay is disabled by default on some removable drive types, such as floppy disk and network drives, but it is enabled by default on CD-ROM drives.

**Note:** You cannot use this setting to enable Autoplay on computer drives that are disabled by default, such as floppy disk and network drives.
Vulnerability

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

Countermeasure

Configure the Turn off Autoplay setting to Enabled.

Potential Impact

Users will have to manually launch setup or installation programs that are provided on removable media.

Logon

You can configure the prescribed Logon computer settings in the following location within the Group Policy Object Editor:

Computer Configuration\Administrative Templates\System\Logon

Don't display the Getting Started welcome screen at logon

This policy setting hides the welcome screen that Microsoft Windows 2000 Professional and Windows XP Professional displays each time that the user logs on. Users can still display the welcome screen if they select it on the Start menu.

The Don't display the Getting Started welcome screen at logon setting applies only to Windows 2000 Professional and Windows XP Professional. It does not affect the Configure Your Server setting in Windows 2000 Server or Windows Server 2003.

The possible values for the Don't display the Getting Started welcome screen at logon setting are:

• Enabled
• Disabled
• Not Configured

Note: This policy setting appears in both the Computer Configuration and User Configuration nodes. If both settings are configured, the Computer Configuration setting takes precedence over the setting in the User Configuration node.

Vulnerability

The Getting Started welcome screen encourages users to explore the Windows XP desktop. Some organizations want to provide their users with training that is focused on their particular role and job tasks, and to guide their users away from other sources of information.

Countermeasure

Configure the Don't display the Getting Started welcome screen at logon setting to Enabled.

Potential Impact

Users will not see the Getting Started welcome screen when they log on to their computers.
Do not process the legacy run list

The **Do not process the legacy run list** setting causes the run list (a list of programs that Windows XP runs automatically when it starts) to be ignored. The customized run lists for Windows XP 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

The possible values for the **Do not process the legacy run list** setting are:

- Enabled
- Disabled
- Not Configured

**Vulnerability**

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.

**Countermeasure**

Configure the **Do not process the legacy run list** setting to **Enabled**.

**Potential 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.

Do not process the run once list

This policy setting causes the run once list (the list of programs that Windows XP runs automatically when it starts) to be ignored. It differs from the **Do not process the legacy run list** setting in that programs on this list will run one time only the next time the client restarts. Setup and installation programs are sometimes added to this list to complete installations after a client restarts. If you enable this policy setting, attackers cannot use the run-once list to launch rogue applications, which was a common method of attack in the past.

**Note:** Customized run once lists are stored in the registry at the following location:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce

The possible values for the **Do not process the run once list** setting are:

- Enabled
- Disabled
- Not Configured

**Vulnerability**

A malicious user can exploit the run once list to install a program that may compromise the security of Windows XP clients.
Countermeasure

Configure the **Do not process the run once list** setting to **Enabled**.

Potential 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.

Group Policy

To modify how Group Policy is processed, you can configure settings in the following location within the Group Policy Object Editor:

```
Computer Configuration\Administrative Templates\System\Group Policy
```

Internet Explorer Maintenance policy processing

This policy setting determines when Internet Explorer Maintenance policies are updated. It affects all policies that use the Internet Explorer Maintenance component of Group Policy, such as those that are located in **Windows Settings\Internet Explorer Maintenance**. This setting takes precedence over customized settings that the Internet Explorer Maintenance program implemented when it was installed.

If you enable the **Internet Explorer Maintenance policy processing** setting you can use the check boxes that are provided to change the options. There is no impact on the computer if you disable or do not configure this policy setting.

The possible values for the **Internet Explorer Maintenance policy processing** setting are:

- **Enabled** with options for:
  - **Allow processing across a slow network connection.** This option updates the policies even when the update is being transmitted across a slow network connection, such as a telephone line. Updates across slow connections can cause significant delays.
  - **Do not apply during periodic background processing.** This option does not allow the computer to update affected policies in the background while it is in use. Background updates can disrupt the user, cause a program to stop or operate abnormally, and (in rare cases) damage data.
  - **Process even if the Group Policy objects have not changed.** This option updates and reapplies the policies, even if they have not changed. Many policy implementations specify that they are updated only when changed. However, you might want to update unchanged policies, such as reapplying a desired setting in case a user has changed it.

- **Disabled**
- **Not Configured**

Vulnerability

You can enable this setting and select the **Process even if the Group Policy objects have not changed** option to ensure that the policies will be reprocessed even if they
have not changed. This approach will enforce established domain–based policies, even if unauthorized changes are made locally.

**Countermeasure**

Configure the **Internet Explorer Maintenance policy processing** setting to **Enabled**. Then clear both of the check boxes for **Allow processing across a slow network** and **Do not apply during periodic background processing**, and select the check box for **Process even if the Group Policy objects have not changed**.

**Potential Impact**

Group Policies will be reapplied every time they are refreshed, which could have a slight impact on performance.

**IP security policy processing**

This policy setting determines when IP security (IPsec) policies are updated. It affects all policies that use the IPsec component of Group Policy. This policy setting takes precedence over customized settings that the program implemented set when it was installed.

If you enable **IP security policy processing** setting you can use the provided check boxes to change the options. There is no impact to the computer if you disable or do not configure this setting.

The possible values for the **IP security policy processing** setting are:

- Enabled with options for:
  - Allow processing across a slow network connection
  - Do not apply during periodic background processing
  - Process even if the Group Policy objects have not changed
- Disabled
- Not Configured

The **Allow processing across a slow network connection** setting updates the policies even when the update is being transmitted across a slow network connection, such as a telephone line or low-bandwidth WAN link. Updates across slow connections can cause significant delays. The **Do not apply during periodic background processing** setting prevents updates to affected policies in the background while the computer is in use. Background updates can disrupt the user, cause a program to stop or operate abnormally, and, in rare cases, damage data. The **Process even if the Group Policy objects have not changed** setting updates and reapplies the policies even if the policies have not changed. Many policy implementations specify that they are updated only when changed. However, you might want to update unchanged policies periodically to reapply desired settings that may have been changed by users.

**Vulnerability**

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.
Countermeasure

Configure the IP security policy processing setting to Enabled. Then clear the Do not apply during periodic background processing check box, and select the Process even if the Group Policy objects have not changed check box.

Potential Impact

IP security Group Policies will be reapplied every time they are refreshed, which could have a slight impact on performance and could interfere with existing network connectivity.

Registry policy processing

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. This policy setting takes precedence over customized settings that the registry policy program implemented set when it was installed.

If you enable the Registry policy processing setting you can use the check boxes that are provided to change the options. There is no impact to the computer if you disable or do not configure this setting.

The Do not apply during periodic background processing option can be used to ensure that the computer does not update affected policies in the background while it is in use. Background updates can disrupt the user, cause programs to stop or operate abnormally, and (in rare cases) damage data. The Process even if the Group Policy objects have not changed option updates and reapplies the policies even if they have not changed. Many Group Policy implementations specify that they are updated only when changed. However, you might want to update unchanged policies to reapply a desired setting in case a user has changed it.

The possible values for the Registry policy processing setting are:

- Enabled with options for:
  - Do not apply during periodic background processing
  - Process even if the Group Policy objects have not changed
- Disabled
- Not Configured

Vulnerability

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.

Countermeasure

Configure the Registry policy processing setting to Enabled. Then clear the Do not apply during periodic background processing check box, and select the Process even if the Group Policy objects have not changed check box.

Potential Impact

Group Policies will be reapplied every time they are refreshed, which could have a slight impact on performance.
Security policy processing
This policy setting determines when security policies are updated. It takes precedence over customized settings that the security policy program implemented when it was installed.

If you enable the Security policy processing setting you can use the check boxes that are provided to change the options. There is no impact to the computer if you disable or do not configure this setting.

The Do not apply during periodic background processing option can be used to ensure that the computer does not update affected policies in the background while the computer is in use. Background updates can disrupt the user, cause programs to stop or operate abnormally, and (in rare cases) damage data. The Process even if the Group Policy objects have not changed option updates and reapplies the policies even if they have not changed. Many Group Policy implementations specify that they are updated only when changed. However, you might want to update unchanged policies to reapply a desired setting in case a user has changed it.

The possible values for the Security policy processing setting are:

• Enabled with options for:
  • Do not apply during periodic background processing
  • Process even if the Group Policy objects have not changed
• Disabled
• Not Configured

Vulnerability
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.

Countermeasure
Configure the Security policy processing setting to Enabled. Then clear the Do not apply during periodic background processing check box, and select the Process even if the Group Policy objects have not changed check box.

Potential Impact
Group Policies will be reapplied every time they are refreshed, which could have a slight impact on performance.

Remote Assistance
Configure the prescribed Remote Assistance computer settings in the following location within the Group Policy Object Editor:

Computer Configuration\Administrative Templates\System\Remote Assistance
Offer Remote Assistance

This policy setting determines whether a support person or an IT “expert” administrator can offer remote assistance to computer users in your environment without an explicit request for assistance through another channel (such as e-mail or instant messaging).

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 and provide view-only privileges to the workstation. The user has to explicitly click Yes to allow the expert to remotely control the workstation after the Offer Remote Assistance setting is configured to Enabled.

If you enable the Offer Remote Assistance setting you have the following options:

• Allow helpers to only view the computer
• Allow helpers to remotely control the computer

When you configure this 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 using one of the following formats:
   • <Domain Name>\<User Name>
   • <Domain Name>\<Group Name>

If you disable or do not configure the Offer Remote Assistance setting, users or groups will not be able to offer unsolicited remote assistance to computer users in your environment.

Vulnerability

A user might be tricked and accept an unsolicited Remote Assistance offer from a malicious user.

Countermeasure

Configure the Offer Remote Assistance setting to Disabled.

Potential Impact

Help desk and support personnel will not be able to proactively offer assistance, although they can still respond to user assistance requests.

Solicit Remote Assistance

This policy setting determines whether remote assistance may be solicited from the Windows XP computers in your environment. If you enable this setting, users can solicit remote assistance to their workstations from IT “expert” administrators.

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 and provide the expert with view-only privileges to the workstation. The user has to explicitly click Yes to allow the expert to remotely control the workstation.
If you enable the **Solicit Remote Assistance** setting you have the following options to permit remote control of the user computer:

- 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 a user help request remains valid:

- Maximum ticket time (value):
- Maximum ticket time (units): hours, minutes or days

When the ticket (help request) expires, the user must send another request before an expert can connect to the computer. If you disable the **Solicit Remote Assistance** setting, users cannot send help requests and experts cannot connect to their computers.

When the **Solicit Remote Assistance** setting is not configured, users can configure solicited remote assistance through the Control Panel. The following settings are enabled by default through the Control Panel: Solicited remote assistance, Buddy support, and Remote control. The value for the Maximum ticket time is set to 30 days. If you disable this setting, no one will be able to access Windows XP clients across the network.

**Vulnerability**

When the **Solicit Remote Assistance** setting is enabled, users may send remote assistance requests to unauthorized personnel.

**Countermeasure**

Configure the **Solicit Remote Assistance** setting to **Disabled**.

**Potential Impact**

If you configure the **Solicit Remote Assistance** setting to **Disabled**, users cannot request remote assistance from help desk or support staff.
**Error Reporting**

Windows Corporate Error Reporting enables administrators to manage the cabinet files that are created by DW.exe and redirect stop error reports to a local file server. This capability provides an alternative to the direct submittal of information to Microsoft through the Internet. When enough stop error entries are collected, administrators can review the information and submit only the stop error data they think is useful to Microsoft.

With Windows Corporate Error Reporting, administrators can review what the most common types of stop errors that users experience. The information can then be used to educate users about how to avoid potential stop error situations.

You can configure the Error Reporting settings in the following location within the Group Policy Object Editor:

```
Computer Configuration\Administrative Templates\System\Error Reporting
```

**Display Error Notification**

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.

The possible values for the Display Error Notification setting are:

- **Enabled**
- **Disabled**
- **Not Configured**

**Vulnerability**

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.

**Countermeasure**

Configure the Display Error Notification setting to Disabled.

**Potential Impact**

Users will not see error report messages when they are generated.
Report Errors

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.

## Vulnerability

In its default configuration, the Windows Corporate Error Reporting features of Windows XP, Windows Server 2003, 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.

**Countermeasure**

Configure the Report Errors setting to Enabled, and then select the Corporate upload file path option to point to the UNC path for your organization's CER server.

**Note:** For more information about how to create a CER server for your organization, see the Windows Corporate Error Reporting Web site at www.microsoft.com/resources/satech/cer/.

**Potential Impact**

Error reporting will be enabled, and new error reports will be sent to the CER server.

**Internet Communications Management**

Products in the Windows Server 2003 and Windows XP families include a variety of technologies that communicate with the Internet to provide increased ease of use. Browser and e-mail technologies are obvious examples, but there are also technologies such as Automatic Updates that help you obtain the latest software and product information, including bug fixes and security patches. These technologies provide many benefits, but they also involve communication with Internet sites, which administrators might want to control.

You can control this communication through a variety of options built into individual components, into the operating system as a whole, and into server components that are designed to manage configurations across your organization. For example, as an administrator you can use Group Policy to control the way some components communicate. For some components, you can direct all communication to the organization's own internal Web site instead of to an external site on the Internet. Also, in Windows Server 2003 with Service Pack 1 (SP1) you can use Windows Firewall and the Security Configuration Wizard (SCW) to help you control aspects of your configuration such as which services are running and which ports are open.

Microsoft has produced two detailed guides for Internet communications management:

- Introduction to Controlling Communication with the Internet for Windows Server 2003 with SP1 at www.microsoft.com/technet/prodtechnol/windowsserver2003/library/W2K3InternetMgmt/55f681e2-de6f-4d76-81d2-af7f889d66f6.mspx describes how to control Internet communications on computers that run Windows Server 2003 with SP1.
- The Using Windows XP Service Pack 2 In a Managed Environment guide at www.microsoft.com/technet/prodtechnol/winxppro/maintain/intmgmt/01_xpint.mspx describes how to control Internet communications on computers that run Windows XP with SP2.

**Distributed COM**

COM provides computer-wide access control lists (ACLs) that govern access to all call, activation, or launch requests on the computer. You can think about these access controls as an additional access check call that is done against a computer-wide ACL on each call, activation, or launch of any COM server on the computer. This access check is in addition to any access check that is run against the server-specific ACLs. If this access check fails, the call, activation, or launch request is denied. In effect, this check provides a minimum authorization standard that must be passed to access any COM server on the computer. For more information about DCOM, see "Component Object Model" at
Chapter 9: Windows XP and Windows Server 2003 Administrative Templates

235


You can manage the new DCOM security features in Windows XP SP2 and Windows Server 2003 SP1 in the following location within the Group Policy Object Editor:

Computer Configuration\Administrative Templates\Windows Components\System\Distributed COM\Application Compatibility Settings

Common Issues

The two settings in this section share common vulnerability, countermeasure, and potential impact information.

Vulnerability

Improperly written COM components may be attacked across the network, which can result in possible information disclosure, denial of service, or privilege escalation attacks.

Countermeasure

Use the Allow local activation security check exemptions and Define Activation Security Check exemptions settings in conjunction with the DCOM access control mechanisms that are described in Chapter 5 to impose access and execution controls on DCOM components.

Potential Impact

If you add DCOM access controls to existing applications, those applications may not run properly.

Allow local activation security check exemptions

This policy setting allows you to specify that local computer administrators can supplement the Define Activation Security Check exemptions list (see the following setting) with activation security checks that take place on the local computer. If you enable this policy setting and DCOM does not find an explicit entry for a DCOM server application ID (AppID) in the Define Activation Security Check exemptions policy, DCOM searches for an entry in the locally configured list.

Define Activation Security Check exemptions

This policy setting allows you to view and change a list of DCOM server application IDs (AppIDs) that are exempted from the DCOM Activation security check. (For more information about COM and the AppID key, see “COM Registry Entries” in the COM SDK Documentation on MSDN® at http://go.microsoft.com/fwlink/?LinkId=32831.)

DCOM uses two lists of DCOM server AppIDs to make security decisions. One list is configured through the Define Activation Security Check exemption Group Policy setting, and the other is created by the local computer administrators. The AppID key is one of the registry keys that COM uses; it groups the configuration options for one or more distributed COM objects into one centralized location in the registry. This key includes the AppID named value, which identifies the AppID GUID that corresponds to the named executable.

If you configure the Define Activation Security Check exemption setting, DCOM ignores the second list unless the associated Allow local activation security check exemptions setting is also enabled. You must enclose any DCOM server AppIDs that
you add to the list of DCOM server AppIDs in curly brackets—for example, {b5dcb061-cefb-42e0-a1be-e6a6438133fe}. (This AppID number is intended as an example only.) If you enter a non-existent or improperly formatted AppID, DCOM adds it to the list; it does not check for errors.

If you enable this policy setting, you can view and change the list of DCOM activation security check exemptions that are defined by Group Policy settings.

You can use one of the following values:

- If you add an AppID to this list and set its value to 1, DCOM does not enforce the Activation security check for that DCOM server
- If you add an AppID to this list and set its value to 0, DCOM always enforces the Activation security check for that DCOM server regardless of local settings.

Note: DCOM servers that are added to this exemption list are exempted only if their custom launch permissions do not contain specific Local Launch, Remote Launch, Local Activate, or Remote Activate permissions set to Allow or Deny for any users or groups. The exemptions for DCOM Server AppIDs that you add to this list apply to the 32-bit version and (if present) the 64-bit version of Windows Server 2003.
User Configuration Settings

The settings that are discussed earlier in this chapter apply to computers that are members of an Active Directory domain. The settings in the following sections apply to individual users.

Internet Explorer User Settings

Internet Explorer is the Web browser that is included with Windows XP and Windows Server 2003. You can manage many of its features through Group Policy at the following location within the Group Policy Object Editor:

User Configuration\Administrative Templates\Windows Components\Internet Explorer

Configure Outlook Express

This policy setting allows administrators to enable and disable the ability of Microsoft Outlook® Express users to save or open attachments that could potentially contain viruses. If you select the check box for Block attachments that could contain a virus, users will not be able to open or save attachments that could potentially contain viruses. Also, if you enable this policy setting, users can specify whether to block or accept e-mail attachments in the Internet Options dialog box.

The possible values for the Configure Outlook Express setting are:

- Enabled with the option for:
  - Block attachments that could contain a virus
- Disabled
- Not Configured

Vulnerability

Users who choose to open e-mail attachments could unwittingly execute hostile code, such as a virus or Trojan horse program, that is contained in an attachment.

Countermeasure

Configure the Configure Outlook Express setting to Enabled and select the check box for Block attachments that could contain a virus.

Potential Impact

Users will be unable to open or execute some types of message attachments in Outlook Express.

Disable Changing Advanced page settings

This policy setting prevents user changes to settings on the Advanced tab of the Internet Options dialog box. If you enable this policy setting, users cannot change advanced Internet settings, such as security, multimedia, and printing options and will not be able to select or clear the check boxes on the Advanced tab. If you disable or do not configure this policy setting, users will be able to select or clear options on the Advanced tab.
If you configure the **Disable the Advanced page** setting, you do not need to configure this policy setting—because that setting removes the **Advanced** tab from the interface.

The possible values for **Disable Changing Advanced page settings** are:

- Enabled
- Disabled
- Not Configured

**Vulnerability**

Users could change some of the Internet Explorer security settings, which could enable them to visit a malicious Web site and download or execute hostile code.

**Countermeasure**

Configure **Disable Changing Advanced page settings** to **Enabled**.

**Potential Impact**

Users will not be able to change the settings on the **Advanced** tab of the **Internet Options** dialog box.

**Disable Changing Automatic Configuration Settings**

This policy setting prevents user changes to automatic configuration settings. Automatic configuration is a process that administrators can use to update browser settings periodically. If you enable this policy setting, automatic configuration settings are dimmed and unavailable. The settings are located in the **Automatic Configuration** area of the **Local Area Network (LAN) Settings** dialog box. If you disable or do not configure this policy setting, users can change automatic configuration settings.

If you enable the **Disable the Connections page** setting, the **Connections** tab is removed from Internet Explorer in the Control Panel and its settings override this policy setting (**Disable Changing Automatic Configuration Settings**).

The possible values for **Disable Changing Automatic Configuration Settings** are:

- Enabled
- Disabled
- Not Configured

**Vulnerability**

Users could change some of the Internet Explorer security settings, which could enable users to visit a malicious Web site and download or execute hostile code.

**Countermeasure**

Configure **Disable Changing Automatic Configuration Settings** to **Enabled**.

**Potential Impact**

Users will be unable to change the automatic configuration settings.
Disable Changing Certificate Settings

This policy setting prevents user changes to certificate settings in Internet Explorer. Certificates are used to verify the identity of software publishers. If you enable this policy setting, the settings in the Certificates area on the Content tab in the Internet Options dialog box are dimmed and unavailable. If you disable or do not configure this setting, users can import new certificates, remove approved publishers, and change settings for certificates that have already been accepted.

The Disable the Content page setting (located in User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel) removes the Content tab from Internet Explorer in the Control Panel and its settings override this policy setting (Disable Changing Certificate Settings).

The possible values for Disable Changing Certificate Settings are:

- Enabled
- Disabled
- Not Configured

Caution: If you enable this policy setting, users can still double-click a software publishing certificate (.spc) file and run the Certificate Manager Import Wizard. This wizard enables users to import and configure settings for certificates from software publishers that have not already been configured for Internet Explorer.

Vulnerability

Users could import new certificates, remove approved certificates, or change settings for previously configured ones. Such occurrences could cause approved applications to fail, or unapproved software to be executed.

Countermeasure

Configure Disable Changing Certificate Settings to Enabled.

Potential Impact

Users will be unable to change the certificate settings.

Disable Changing Connection Settings

This policy setting prevents user changes to dial-up settings. If you enable this policy setting, the Settings button on the Connections tab in the Internet Options dialog box is unavailable. If you disable or do not configure this policy setting, users can change their settings for dial-up connections.

If you enable the Disable the Connections page setting (located in User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel) the Connections tab is removed from the Internet Options dialog box and there is no need to configure this policy setting (Disable Changing Connection Settings).

The possible values for Disable Changing Connection Settings are:

- Enabled
- Disabled
- Not Configured
**Vulnerability**

Users could alter existing connections to make it impossible for them to use Internet Explorer to browse some, or all, Web sites.

**Countermeasure**

Configure **Disable Changing Connection Settings** to **Enabled**.

**Potential Impact**

Users will be unable to change the connection settings.

**Disable Changing Proxy Settings**

This policy setting prevents user changes to proxy settings. If you enable this policy setting, the proxy settings are dimmed and unavailable. These settings are located in the **Proxy Server** area of the **Local Area Network (LAN) Settings** dialog box, which appears when the user clicks the **Connections** tab and then **LAN Settings** on the **Internet Options** dialog box.

If you enable the **Disable the Connections page** setting (located in `\User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel`) you do not need to configure this policy setting (**Disable Changing Proxy Settings**) because the **Disable the Connections page** setting removes the **Connections** tab from the **Internet Options** dialog box.

The possible values for **Disable Changing Proxy Settings** are:

- **Enabled**
- **Disabled**
- **Not Configured**

**Vulnerability**

Users could alter existing proxy server settings and make it impossible for them to use Internet Explorer to browse some, or all, Web sites.

**Countermeasure**

Configure **Disable Changing Proxy Settings** to **Enabled**.

**Potential Impact**

Users will be unable to change the proxy settings.

**Disable Internet Connection Wizard**

This policy setting controls the ability of users to run the Internet Connection Wizard (ICW). If you enable this setting, the **Setup** button on the **Connections** tab of the **Internet Options** dialog box is dimmed and unavailable. This policy setting also prevents execution of the wizard in other ways; for example, users will not be able to click the **Connect to the Internet** icon on the desktop or click **Start**, **Programs**, **Accessories**, **Communications**, and then **Internet Connection Wizard**. If you disable or do not configure this policy setting, users can change their connection settings by means of the ICW.
The possible values for the Disable Internet Connection Wizard setting are:

- Enabled
- Disabled
- Not Configured

**Note:** This policy setting overlaps with the Disable the Connections page setting (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), which removes the Connections tab from the Internet Options dialog box. However, if you use this setting, users can still run the ICW from the desktop or the Start menu.

**Vulnerability**

Users could run the ICW and create a new dial-up or network connection, which could expose the organization's network to access by unauthorized users through the new, unmanaged connection.

**Countermeasure**

Configure the Disable Internet Connection Wizard setting to Enabled.

**Potential Impact**

Users will be unable to run the ICW.

**Do not allow AutoComplete to save passwords**

This policy setting disables automatic completion of user names and passwords in forms on Web pages, and prevents the display of "save password" prompts to users. If you enable this policy setting, the check boxes for User Names and Passwords on Forms and Prompt Me to Save Passwords are dimmed and unavailable. (To display these check boxes, users open the Internet Options dialog box, click the Content tab, and then click AutoComplete.) If you disable or do not configure this setting, users can determine whether Internet Explorer automatically completes user names and passwords on forms, and prompts them to save passwords.

The Disable the Content page setting (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel) removes the Content tab from Internet Explorer in Control Panel, and therefore takes precedence over this (Do not allow AutoComplete to save passwords) policy setting.

The possible values for The Do not allow AutoComplete to save passwords setting are:

- Enabled
- Disabled
- Not Configured

**Vulnerability**

Although the AutoComplete feature is very useful, it loads passwords into Protected Storage. Protected Storage is a very secure mechanism, the information that is stored there must be accessible to the user who saved it. Tools have been released on the Internet that can view the contents of a user's Protected Storage. These tools only work when they are executed by a user to view their Protected Storage, and cannot be used to view another user's Protected Storage or password. A user who unknowingly executes one of these tools could expose their password to an attacker.
Countermeasure

Configure the Do not allow AutoComplete to save passwords setting to Enabled.

Potential Impact

Users will be unable to use the AutoComplete feature to save passwords.

Internet Control Panel

You can manage Internet-related settings through the Internet Control Panel applet. Availability of the applet's features can be controlled through the Internet Control Panel node in Group Policy. These policy settings can be configured in the following location within the Group Policy Object Editor:

User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel

Disable the Advanced Page

This policy setting removes the Advanced tab from the Internet Options dialog box. If you enable this policy setting, users cannot view or change advanced Internet settings such as security, multimedia, and printing options. If you disable or do not configure this policy setting, users can view and change these settings.

When this policy setting is enabled, you do not need to enable the Disable changing Advanced page setting (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer) because the Advanced tab is removed from the Internet Options dialog box.

The possible values for the Disable the Advanced Page setting are:

- Enabled
- Disabled
- Not Configured

Vulnerability

Users could change some of the Internet Explorer security settings, which could enable them to visit a malicious Web site and download or execute hostile code.

Countermeasure

Configure the Disable the Advanced Page setting to Enabled.

Potential Impact

Users will be unable to view the Advanced dialog box.

Disable the Security Page

This policy setting removes the Security tab from the Internet Options dialog box. If you enable this setting, users cannot view or change settings for security zones, such as those for scripting, downloads, and user authentication. If you disable or do not configure this setting, users can view and change these settings.
The possible values for the **Disable the Security Page** setting are:

- Enabled
- Disabled
- Not Configured

When you configure this setting, you do not need to configure the following Internet Explorer settings (because the Security tab is removed from the **Internet Options** dialog box):

- Security zones: **Do not allow users to change policies**
- Security zones: **Do not allow users to add/delete sites**

**Vulnerability**

Users could change some of the Internet Explorer security settings, which could enable them to visit a malicious Web site and download or execute hostile code.

**Countermeasure**

Configure the **Disable the Security Page** setting to **Enabled**.

**Potential Impact**

Users will be unable to view the Security Page.

**Offline Pages**

Internet Explorer can download and cache pages to make them available for offline use. This feature can be controlled through the Offline Pages node in Group Policy. These policy settings can be configured in the following location within the Group Policy Object Editor:

```
User Configuration\Administrative Templates\Windows Components\Internet Explorer\Offline Pages
```

**Disable adding channels**

This policy setting can remove users’ ability to add channels to Internet Explorer. Channels are Web sites that are updated automatically on your computer by means of a schedule that is specified by the channel provider.

If you enable this policy setting, the **Add Active Channel** button that users click to subscribe to channels is disabled. Users also cannot add content that is based on a channel, such as some of the Active Desktop® items from the Microsoft Active Desktop Gallery, to their desktop. If you disable or do not configure this setting, users can add channels to the Channel tool bar or to their desktop.

The possible values for the **Disable adding channels** setting are:

- Enabled
- Disabled
- Not Configured
**Vulnerability**

Data could be sent to a user's browser without any direct interaction by the user. That is, the browser could download Web content that is not directly requested by the user.

**Countermeasure**

Configure the **Disable adding channels** setting to **Enabled**.

**Potential Impact**

Users will not be able to add channels.

**Disable adding schedules for offline pages**

This policy setting is intended for organizations that are concerned about server load. You can use it to control users’ ability to specify that Web pages can be downloaded and viewed offline when their computer is not connected to the Internet.

If you enable this policy setting, users cannot add new schedules to download offline content. The **Make Available Offline** check box dims and becomes unavailable in the **Add Favorite** dialog box. If you disable or do not configure this policy setting, users can add new offline content schedules. The **Hide Favorites menu** setting (located in User Configuration\Administrative Templates\Windows Components\Internet Explorer) takes precedence over this policy setting.

The possible values for the **Disable adding channels** setting are:

- Enabled
- Disabled
- Not Configured

**Vulnerability**

Data could be sent to a user's browser without any direct interaction by the user. That is, the browser could download Web content that is not directly requested by the user.

**Countermeasure**

Configure the **Disable adding schedules for offline pages** setting to **Enabled**.

**Potential Impact**

Users will not be able to add schedules for offline pages.

**Disable all scheduled offline pages**

This policy is intended for organizations that are concerned about server load. You can use it to disable schedules that currently exist to download Web pages so that they can be viewed offline. When users make Web pages available to view offline, they can view the pages when their computer is not connected to the Internet.

If you enable this policy setting, the check boxes for schedules on the **Schedule** tab of the **Web page properties** dialog box are cleared and users cannot select them. (To display this tab, users click **Tools** and then **Synchronize**, select a Web page, click **Properties**, and then click the **Schedule** tab.) If you disable this policy setting, Web pages can be updated according to schedules that are specified on the **Schedule** tab. The **Hide Favorites menu** setting (located in User Configuration\Administrative...
Templates\Windows Components\Internet Explorer) takes precedence over this setting.

The possible values for the **Disable adding channels** setting are:

- Enabled
- Disabled
- Not Configured

**Vulnerability**

Data could be sent to a user's browser without any direct interaction by the user. That is, the browser could download Web content not directly requested by the user.

**Countermeasure**

Configure the **Disable all scheduled offline pages** setting to **Enabled**.

**Potential Impact**

Users will not be able to view any of the scheduled offline pages.

**Disable channel user interface completely**

This policy setting controls whether users can view the Channel interface. Channels are Web sites that are automatically updated on a user's computer by means of a schedule that is specified by the channel provider.

If you enable this policy setting, the Channel user interface (UI) is disabled and users cannot select the **Internet Explorer Channel Bar** check box on the **Web** tab of the **Display Properties** dialog box. If you disable or do not configure this setting, users can view and subscribe to channels through the Channel interface.

The possible values for the **Disable channel user interface completely** setting are:

- Enabled
- Disabled
- Not Configured

**Vulnerability**

Data could be sent to a user's browser without any direct interaction by the user. That is, the browser could download Web content not directly requested by the user.

**Countermeasure**

Configure the **Disable channel user interface completely** setting to **Enabled**.

**Potential Impact**

Users will not be able to access the channel UI.

**Disable downloading of site subscription content**

This policy setting controls whether users can download content from Web sites to which they subscribe. This capability allows users to view Web pages when they are offline (when their computer is not connected to the Internet).
If you enable this policy setting, users cannot download content from Web sites to which they subscribe. However, synchronization with the Web pages will still occur to determine if any content was updated since the last time the user synchronized with, or visited, the page. If you disable or do not configure this policy setting, users can download content.

The **Disable downloading of site subscription content** setting and the **Hide Favorites menu** setting (located in User Configuration\Administrative Templates\Windows Components\Internet Explorer) override this policy setting.

The possible values for the **Disable downloading of site subscription content** setting are:

- Enabled
- Disabled
- Not Configured

**Vulnerability**

Data could be sent to a user's browser without any direct interaction by the user. That is, the browser could download Web content that was not directly requested by the user.

**Countermeasure**

Configure the **Disable downloading of site subscription content** setting to **Enabled**.

**Potential Impact**

Users will not be able to automatically download content through site subscriptions.

**Disable editing and creating of schedule groups**

This policy setting controls whether users can add, edit, or remove schedules to download content so that Web pages and groups of Web pages to which users subscribe can be viewed offline. A favorite Web page and the Web pages that it links to comprise a subscription group.

If you enable this policy, the **Add**, **Remove**, and **Edit** buttons on the **Schedule** tab of the Web page **Properties** dialog box are dimmed and unavailable. (To display this tab, users click **Tools**, **Synchronize**, select a Web page, click the **Properties** button, and then the **Schedule** tab.) If you disable or do not configure this setting, users can add, remove, and edit schedules for Web sites and Web site groups.

The **Disable editing schedules for offline pages** setting and the **Hide Favorites menu** setting (located in User Configuration\Administrative Templates\Windows Components\Internet Explorer) override this policy.

The possible values for the **Disable editing and creating of schedule groups** setting are:

- Enabled
- Disabled
- Not Configured

**Vulnerability**

Data could be sent to a user's browser without any direct interaction by the user. That is, the browser could download Web content that is not directly requested by the user.
Chapter 9: Windows XP and Windows Server 2003 Administrative Templates

Countermeasure

Configure the Disable editing and creating of schedule groups setting to Enabled.

Potential Impact

Users will not be able to add, edit, or remove schedules to download Web page content so that it can be viewed offline.

Disable editing schedules for offline pages

This policy setting is intended for organizations that are concerned about server load. It controls whether users can edit schedules that already exist to download Web pages so that they can be viewed offline (when their computer is not connected to the Internet).

If you enable this policy setting, users cannot display the schedule properties of pages that are configured to be viewed offline. If users click Tools and then Synchronize, select a Web page, and then click the Properties button, no properties will display. No alert is displayed that states the option is unavailable. If you disable or do not configure this policy setting, users can edit existing schedules to download Web content so that it can be viewed offline.

The Hide Favorites menu setting (located in User Configuration\Administrative Templates\Windows Components\Internet Explorer) takes precedence over this policy setting.

The possible values for the Disable editing schedules for offline pages setting are:

- Enabled
- Disabled
- Not Configured

Vulnerability

Data could be sent to a user's browser without any direct interaction by the user. That is, the browser could download Web content that is not directly requested by the user.

Countermeasure

Configure the Disable editing schedules for offline pages setting to Enabled.

Potential Impact

Users will not be able to edit schedules that control when Web page content can be downloaded so that it can be viewed offline.

Disable offline page hit logging

This policy setting controls whether channel providers can record information about when their channel pages are viewed by users who work offline.

If you enable this policy setting, any channel logging settings that are configured by channel providers in the channel definition format (.cdf) file are disabled. The .cdf file determines the schedule and other settings for Web content downloads. If you disable or do not configure this policy setting, channel providers can record information about when their channel pages are viewed by users who work offline.
The possible values for the **Disable offline page hit logging** setting are:

- Enabled
- Disabled
- Not Configured

**Vulnerability**

Data could be sent to a user's browser without any direct interaction by the user. That is, the browser could download Web content that is not directly requested by the user.

**Countermeasure**

Configure the **Disable offline page hit logging** setting to **Enabled**.

**Potential Impact**

Users who access content offline will not have their page hits forwarded to the Web site the next time they are online.

**Disable removing channels**

This policy setting is intended to help administrators ensure that users' computers are updated uniformly across their organization. It controls whether users can disable channel synchronization in Internet Explorer. Channels are Web sites that are automatically updated on your computer in accordance with a schedule that is specified by the channel provider.

If you enable this policy setting, users cannot interfere with channel synchronization. If you disable or do not configure this policy setting, users can disable channel synchronization.

The possible values for the **Disable removing channels** setting are:

- Enabled
- Disabled
- Not Configured

**Note**: This policy setting does not prevent users' ability to remove active content from the desktop interface.

**Vulnerability**

Data could be sent to a user's browser without any direct interaction by the user. That is, the browser could download Web content that is not directly requested by the user.

**Countermeasure**

Configure the **Disable removing channels** setting to **Enabled**.

**Potential Impact**

Users will not be able to remove channels or prevent channel synchronization.
Disable removing schedules for offline pages

This policy setting is intended for organizations that are concerned about server load. It controls whether users can clear preconfigured setting restrictions for Web page downloads so that they can be viewed offline (when their computer is not connected to the Internet).

If you enable this policy setting, the checkbox for Make Available Offline in the Organize Favorites dialog box and the Make This Page Available Offline check box are dimmed and unavailable (although they remain selected). (To display the Make This Page Available Offline check box, users click Tools, Synchronize, and then Properties.) If you disable or do not configure this policy setting, users can remove preconfigured setting restrictions on pages to download them so that they can be viewed offline.

The Hide Favorites menu setting (located in User Configuration\Administrative Templates\Windows Components\Internet Explorer) takes precedence over this setting.

The possible values for the Disable removing schedules for offline pages setting are:

- Enabled
- Disabled
- Not Configured

Vulnerability

Data could be sent to a user's browser without any direct interaction by the user. That is, the browser could download Web content that is not directly requested by the user.

Countermeasure

Configure the Disable removing schedules for offline pages setting to Enabled.

Potential Impact

Users will not be able to remove schedules for offline pages.
**Browser Menus**

Individual features in the Internet Explorer menu system can be enabled and disabled through the Browser Menus node in Group Policy. These policy settings can be configured in the following location within the Group Policy Object Editor:

```
User Configuration\Administrative Templates\Windows Components\Internet Explorer\Browser menus
```

**Disable Save this program to disk option**

If you enable this policy setting, users cannot click the **Save This Program to Disk** button to download program files. Users will be informed that the command is not available. If you disable or do not configure this setting, users can download programs from their browsers.

Possible values for the **Browser menus: Disable Save this program to disk option** setting are:

- Enabled
- Disabled
- Not Configured

**Vulnerability**

Users could download and execute hostile code from Web sites.

**Countermeasure**

Configure the **Disable Save this program to disk** option setting to **Enabled**.

**Potential Impact**

Users will be unable to click the **Save This Program to Disk** button to download program files.

**Persistence Behavior**

Internet Explorer allows dynamic HTML (DHTML) objects to save their settings or data to disk; the term for this capability is persistence. Form data, styles, state, and script variables can be persisted in the current session's memory stream, in the favorites list, in HTML, or in XML. The four DHTML persistence behaviors are saveFavorite, saveHistory, saveSnapshot, and userData. Internet Explorer allows you to apply controls, by security zone, to the amount of data that applications can save by using this mechanism.

The possible values for the **Persistence Behavior** setting are:

- Enabled
  - Per domain (in kilobytes). This configuration controls how much total data can be saved by scripts that are associated with a given domain.
  - Per document (in kilobytes). This configuration controls how much total data can be saved by DHTML constructs in a specific Web page.
- Disabled
- Not Configured
Chapter 9: Windows XP and Windows Server 2003 Administrative Templates  251

Vulnerability

A malicious Web page can covertly save malicious data, or excessive amounts of data, on a target computer.

Countermeasure

Enable per-security zone size limits for the Internet and Restricted Sites zones.

Potential Impact

None.

Attachment Manager

In Windows Server 2003 SP1 and Windows XP SP2, a new service called Attachment Manager provides a consistent set of behaviors for file attachments in e-mail messages and Web pages. The Attachment Manager service implements a uniform set of prompts that are used for file downloads, mail attachments, shell process execution, and program installation. These prompts have been modified to be clearer and more consistent than they were in previous versions of Windows. Also, the publisher information will display before a file type that is signable and that could potentially harm the user’s computer is opened. (Common examples of signable file types that can potentially harm computers are .exe, .dll, .ocx, .msi, and .cab.) The Attachment Manager service includes a new application programming interface (API) that allows application developers to make use of this new user interface.

The Attachment Manager service classifies files that you receive or that you download based on the file type and the file name extension. The service classifies files as high risk, medium risk, and low risk. When you save files to your hard disk from a program that uses the Attachment Manager service, the Web content zone information for the file is also saved with the file. For example, if you save a compressed file (.zip) that is attached to an e-mail message, the Web content zone information is also saved and you will not be able to extract the contents from the compressed file.

Note: The Web content zone information is saved together with the files only if the computer uses the NTFS file system.

The Attachment Manager service divides files into three classes:

• **High Risk.** If the attachment is in the list of high risk file types and is from the restricted zone, Windows blocks user access to the file. If the file is from the Internet zone, Windows prompts the user before it allows access to the file.

• **Moderate Risk.** If the attachment is in the list of moderate risk file types and is from the restricted or Internet zone, Windows prompts the user before it allows access to the file.

• **Low Risk.** If the attachment is in the list of low risk file types, Windows will not prompt the user before it allows access to the file, regardless of the file’s zone information.

These policy settings can be configured in the following location within the Group Policy Object Editor:

User Configuration\Administrative Templates\Windows Components\Attachment Manager
Default risk level for file attachments

This policy setting allows you to manage the default risk level for file types. To fully customize the risk level for file attachments, you may also need to configure the trust logic for file attachments. If you enable this policy setting, you can specify the default risk level for file types that are not explicitly included in the high, medium, or low risk type lists. If you disable or do not configure this policy setting, Windows sets the default risk level to moderate.

The possible values for the Default risk level for file attachments setting are:
- Enabled, with options to configure the default risk level to
  - High Risk
  - Moderate Risk
  - Low Risk.
- Disabled
- Not Configured

Vulnerability
An attacker might disguise malicious code to trick users and cause them to execute it.

Countermeasure
Configure the Default risk level for file attachments setting to Enabled: Moderate Risk.

Potential Impact
Users will have to answer security prompts before they can access files whose types aren't explicitly included on the low-risk file type list.

Inclusion list for high risk file types

This policy setting allows you to configure the list of high risk file types. If the file attachment is in the list of high risk file types and is from the restricted zone, Windows blocks user access to the file. If the file is from the Internet zone, Windows prompts the user before it allows access to the file. This inclusion list takes precedence over the Medium and Low risk inclusion lists when an extension is listed in more than one inclusion list. If you enable this policy setting, you can create a custom list of high risk file types. If you disable or do not configure this policy setting, Windows uses its built-in list of high risk file types.

The possible values for the Inclusion list for high risk file types setting are:
- Enabled (allows you to specify a comma-separated list of file extensions)
- Disabled
- Not Configured

Vulnerability
Users might accidentally open a high-risk file, which could compromise their computers and possibly other computers on the network.
**Countermeasure**

Configure the *Inclusion list for high risk file types* setting to *Enabled* and specify the additional file types that you want to control.

**Potential Impact**

If a file type is listed on more than one inclusion list, the most restrictive list will apply. When you define a value for this setting, it overrides the built-in Windows high-risk file type inclusion list.

**Inclusion list for moderate risk file types**

This policy setting allows you to configure the list of moderate risk file types. If the attachment is in the list of moderate risk file types and is from the restricted or Internet zone, Windows prompts the user before it allows access to the file. This inclusion list overrides the built-in list of potentially high risk file types and it takes precedence over the Low risk inclusion list, but it has a lower precedence than the High risk inclusion list. If you enable this policy setting, you can specify file types that pose a moderate risk. If you disable or do not configure this policy setting, Windows uses its default trust logic.

The possible values for the *Inclusion list for moderate risk file types* setting are:

- **Enabled** (allows you to specify a comma-separated list of file extensions)
- **Disabled**
- **Not Configured**

**Vulnerability**

Users might accidentally open a high-risk file, which could compromise their computers and possibly other computers on the network.

**Countermeasure**

Configure the *Inclusion list for moderate risk file types* setting to *Enabled* and specify the additional file types that you want to control.

**Potential Impact**

If a file type is listed on more than one inclusion list, the most restrictive list will apply. When you define a value for this policy setting, it overrides the built-in Windows moderate risk file type inclusion list. Use caution when you move high risk file types such as .EXE to the moderate risk inclusion list, because it will then be easier for users to execute potentially risky files.

**Inclusion list for low file types**

This policy setting allows you to configure the list of low risk file types. If the attachment is in the list of low risk file types, Windows will not prompt the user before it allows access to the file, regardless of the file's zone information. This inclusion list overrides the built-in Windows list of high risk file types and has a lower precedence than the High or Medium risk inclusion lists. If you enable this policy setting, you can specify file types that pose a low risk. If you disable or do not configure this policy setting, Windows uses its default trust logic.
The possible values for the **Inclusion list for low file types** setting are:

- **Enabled** (allows you to specify a comma-separated list of file extensions)
- **Disabled**
- **Not Configured**

**Vulnerability**

Users might accidentally open a high-risk file type, which could compromise their computers and possibly other computers on the network.

**Countermeasure**

Configure the **Inclusion list for moderate risk file types** setting to **Enabled** and specify the additional file types that you want to control.

**Potential Impact**

If a file type is listed on more than one inclusion list, the most restrictive list will apply. When you define a value for this policy setting, it overrides the built-in Windows low risk file type inclusion list. Use caution when you move high risk file types such as .EXE to the low risk inclusion list, because it will then be easier for users to execute potentially risky files.

**Trust logic for file attachments**

This policy setting allows you to configure the logic that Windows uses to determine the risk for file attachments. If you enable this policy setting, you can choose the order in which Windows processes risk assessment data. If you disable or do not configure this policy setting, Windows uses its default trust logic, which prefers the file handler over the file type.

The possible values for the **Trust logic for file attachments** setting are:

- **Enabled**, with the following options:
  - **Looking at the file handler and type**. When this option is selected, Windows will use the file handler data or the file type data, whichever is more restrictive.
  - **Preferring the file handler**. When this option is selected, Windows will always trust the file handler (for example, notepad.exe) no matter what the file type is.
  - **Preferring the file type**. When this option is selected, Windows will always trust the file type no matter what the file handler is.
- **Disabled**
- **Not Configured**

**Vulnerability**

An attacker might craft a file to exploit a vulnerability in a specific file handler.

**Countermeasure**

Configure the **Trust logic for file attachments** setting to **Enabled: Looking at the file handler and type**.
Potential Impact

When you configure the Trust logic for file attachments setting to use both the file handler and type, users will see more attachment security prompts display because Windows will always use the most restrictive scope to make attachment security decisions.

Do not preserve zone information in file attachments

This policy setting allows you to manage whether Windows marks file attachments with information about their zone of origin (restricted, Internet, intranet, local). It requires NTFS to function correctly, and will fail without notice on a FAT32 file system. If the zone information is not preserved, Windows cannot make proper risk assessments. If you enable this policy setting, Windows does not mark file attachments with their zone information. If you disable or do not configure this policy setting, Windows marks file attachments with their zone information.

The possible values for the Do not preserve zone information in file attachments setting are:

• Enabled
• Disabled
• Not Configured

Vulnerability

A file that is downloaded from a computer in the Internet or Restricted Sites zone may be moved to a location that makes it appear safe, like an intranet file share, and executed by an unsuspecting user.

Countermeasure

Configure the Do not preserve zone information in file attachments setting to Enabled.

Potential Impact

None.

Hide mechanisms to remove zone information

This policy setting allows you to manage whether users can manually remove the zone information from saved file attachments. Typically, they can click the Unblock button in the file’s Properties sheet or use a check box in the Security Warning dialog. If they can remove the zone information, users could open potentially dangerous file attachments that Windows had previously blocked. If you enable this policy setting, Windows hides the checkbox and the Unblock button. If you disable or do not configure this policy setting, Windows displays the checkbox and Unblock button.

The possible values for the Hide mechanisms to remove zone information setting are:

• Enabled
• Disabled
• Not Configured
**Vulnerability**
A user might remove information that indicates a file came from an untrustworthy location.

**Countermeasure**
Configure the Hide mechanisms to remove zone information setting to Enabled.

**Potential Impact**
Users who have a legitimate need to remove zone information from files will not be able to do so.

**Notify antivirus programs when opening attachments**
This policy setting allows you to manage how registered antivirus programs are notified when attachments are opened. If multiple programs are registered, they will all be notified. If the registered antivirus program already performs on-access checks or scans files as they arrive on the computer’s e-mail server, additional calls would be redundant. If you enable this policy setting, Windows calls the registered antivirus programs so that they can scan any file attachment that the user opens. If the antivirus program fails, the attachment is blocked from being opened. If you disable or do not configure this policy setting, Windows does not call the registered antivirus programs when file attachments are opened.

The possible values for the Notify antivirus programs when opening attachments setting are:
- Enabled
- Disabled
- Not Configured

**Vulnerability**
Antivirus programs that do not perform on-access checks may not be able to scan downloaded files.

**Countermeasure**
Configure the Notify antivirus programs when opening attachments setting to Enabled.

**Potential Impact**
When the Notify antivirus programs when opening attachments setting is Enabled, every downloaded file or e-mail attachment that the user opens will be scanned.
Windows Explorer

Windows Explorer is used to navigate the file system on clients that run Windows XP Professional.

You can configure the prescribed Windows Explorer user settings in the following location within the Group Policy Object Editor:

User Configuration\Administrative Templates\Windows Components\Windows Explorer

Remove CD Burning features

This policy setting removes the built-in CD burning features in Windows XP. Windows XP allows you to create and modify rewritable CDs if you have a read/write CD drive connected to your computer. This feature can be used to copy large amounts of data from a hard drive to a CD, which can then be removed from the computer.

**Note:** This policy setting does not prevent the ability of third-party applications to create or modify CDs with a CD writer. This guide recommends that you use software restriction policies to deny third-party applications the ability to create or modify CDs. For more information, see Chapter 6, “Software Restriction Policy for Windows XP Clients.”

Another way to prevent users from CD burning is to remove the CD writers from the client computers in your environment and replace them with read-only CD drives, or remove them all together.

**Vulnerability**

The built-in CD burning feature can be used to surreptitiously copy information that resides on the computer or on the network.

**Countermeasure**

Configure the **Remove the CD Burning features** setting to **Enabled**.

**Potential Impact**

When the **Remove CD Burning features** setting is **Enabled**, no CDs can be written without the use of third-party applications.

Remove Security tab

This policy setting disables the Security tab on the file and folder properties dialog boxes in Windows Explorer. If you enable this policy setting, users cannot access the Security tab (after they open the Properties dialog box) for all file system objects, including folders, files, shortcuts, and drives. Users will not be able to change settings on the Security tab or view the list of users.

**Vulnerability**

Users can access the Security tab to determine which accounts have permissions for any file system object. Attackers can target those accounts to gain greater access.

**Countermeasure**

Configure the **Remove Security tab** setting to **Enabled**.
Potential Impact

When the Remove Security tab setting is Enabled, users will not be able to view the Security tab for file system objects, review permissions, or make permission changes through Windows Explorer.

System

You can configure the prescribed System user setting in the following location within the Group Policy Object Editor:

User Configuration\Administrative Templates\System

Prevent access to registry editing tools

This policy setting disables the Windows registry editors Regedit.exe and Regedt32.exe. If you enable this policy setting, a message will display when the user tries to start a registry editor that states they cannot use either of these editors. This policy setting denies registry access with these tools to users or intruders but does not prevent access to the registry itself.

Vulnerability

Users may try to use registry editing tools to bypass other restrictions and policies. Although many of the settings that are applied by Group Policy cannot be bypassed in this fashion, settings that are directly applied to the registry can be modified this way.

Countermeasure

Configure the Prevent access to registry editing tools setting to Enabled.

Potential Impact

When the Prevent access to registry editing tools setting is Enabled, users cannot launch Regedit.exe or Regedt32.exe to make changes to the registry.

System\Power Management

You can configure the prescribed System\Power Management user setting in the following location within the Group Policy Object Editor:

User Configuration\Administrative Templates\System\Power Management

Prompt for password on resume from hibernate / suspend

This policy setting controls whether client computers in your environment are locked when they resume from a hibernated or suspended state. If you enable this setting, client computers are locked when they resume operation and users must enter their passwords to unlock them. If you disable or do not configure this setting there is a potential for a serious security breach, because the client computers may be accessed by anyone after they resume operation.
**Screen Saver Settings**

Screen savers were originally developed to protect cathode ray–based computer monitors from image burn-in on their screens. They have since evolved into another way for users to customize the appearance and behavior of their computer’s virtual desktop. Screen savers have also become a security tool; with the advent of screen savers that automatically lock the desktop, they have become a useful way to additionally protect unattended end-user computers when users forget to lock their console.

You can configure the prescribed Screen Saver settings in the following location within the Group Policy Object Editor:

```
User Configuration\Administrative Templates\Control Panel\Display
```

**Hide Screen Saver tab**

This policy setting determines whether users can add, configure, or change the screen saver on the computer.

If you enable this policy setting, the Screen Saver tab is removed from Display in Control Panel and users will not be able to make any changes to the screen saver settings. If you disable or do not configure this policy setting, users will have access to this tab.

The possible values for the Hide Screen Saver tab setting are:

- Enabled
- Disabled
- Not Configured

**Vulnerability**

Users may change the settings on their screen savers to remove passwords or lengthen the amount of time before a screen saver locks the computer.

**Countermeasure**

Configure the Hide Screen Saver tab setting to Enabled.

**Potential Impact**

Users will not be able to change screen saver settings.

**Password protect the screen saver**

This policy setting determines whether screen savers that are used on the computer are password-protected.

If you enable this policy setting, all screen savers are password-protected. If you disable this policy setting, password protection cannot be set on any screen saver. This configuration also disables the Password protected check box on the Screen Saver tab of the Display in Control Panel dialog box, which offers another way to prevent user changes to the password protection setting.

If you do not configure this policy setting, users can choose whether or not to set password protection on each screen saver on their computers. To ensure that a computer will be password-protected, this guide recommends that you enable the Screen Saver setting and then specify a timeout with the Screen Saver timeout setting.
The possible values for the **Password protect the screen saver** setting are:

- **Enabled**
- **Disabled**
- **Not Configured**

**Note:** To remove the **Screen Saver** tab, use the **Hide Screen Saver tab** setting.

**Vulnerability**

Screen savers without password protection will fail to lock the console for users who leave their computers unattended.

**Countermeasure**

Configure the **Password protect the screen saver** setting to **Enabled**.

**Potential Impact**

Users will have to unlock their computers after the screen saver launches.

**Screen Saver**

This policy setting enables desktop screen savers to work. If you disable this policy setting, screen savers cannot run.

If you do not configure this policy setting, there is no effect on the computer. If you enable this policy setting, screen savers can run if the following two conditions are met:

- A valid screensaver on the client is specified through the Screensaver executable name setting or in Control Panel on the client computer.
- The screensaver timeout is set to a non-zero value through the setting or in Control Panel.

The possible values for the **Screen Saver** setting are:

- **Enabled**
- **Disabled**
- **Not Configured**

**Vulnerability**

This policy setting must be enabled to use the locking screensaver feature described earlier.

**Countermeasure**

Configure the **Screen Saver** setting to **Enabled**.

**Potential Impact**

This policy setting enables screen savers for user computers in your environment.

**Screen Saver executable name**

This policy setting specifies the screen saver that displays on the user's desktop. If you enable this policy setting, the computer displays the specified screen saver on the user's desktop and disables the drop-down list of screen savers on the **Screen Saver** tab of the
Display in Control Panel dialog box (to prevent user changes). If you disable or do not configure this policy setting, users can select any screen saver.

To enable the Screen Saver executable name setting
1. Enter the name of the file that contains the screen saver. Include the .scr file name extension.
2. If the screen saver file is not in the %Systemroot%\System32 folder, type the fully qualified path to the file.
   If the specified screen saver is not installed on a computer to which this setting applies, the setting is ignored.

The possible values for the Screen Saver executable name setting are:
• Enabled. After this value is specified, enter the name of the screen saver executable.
• Disabled
• Not Configured

Note: This policy setting can be superseded by the Screen Saver setting. If you disable the Screen Saver setting, the screen saver executable name setting is ignored and screen savers will not run.

Vulnerability
For the locking screensaver feature to function, a valid screen saver executable must be specified.

Countermeasure
Configure the Screen Saver executable name setting to Scrnsave.scr—the blank screen saver—or some other screen saver executable.

Potential Impact
The blank screen saver, or whatever screen saver is specified, will execute when the screen saver timeout is reached.

Screen Saver timeout
This policy setting specifies how much user idle time must elapse before the screen saver launches. When configured, this idle time can be set from a minimum of 1 second to a maximum of 86,400 seconds, or 24 hours. If you configure this setting to 0, the screen saver will not start.

This policy setting has no effect in any of the following circumstances:
• If the policy setting is Disabled or Not Configured.
• If the wait time is set to 0.
• If the No screen saver setting is enabled.
• If neither the Screen saver executable name setting or the Screen Saver tab on the client computer's Display Properties dialog box specifies a valid, existing screensaver program on the client computer.

When not configured, whatever wait time is set on the client through the Screen Saver tab of the Display Properties dialog box is used. The default is 15 minutes.
The possible values for the Screen Saver timeout setting are:

- Enabled, with a screen saver time-out ranging between 1 and 86,400 seconds.
- Disabled
- Not Configured

Vulnerability

You must configure a valid screen saver timeout for the locking screensaver feature to work.

Countermeasure

Configure the Screen Saver timeout setting to an appropriate value for your organization's security requirements.

Potential Impact

The screen saver will execute after a period of inactivity.
More Information

The following links provide additional information about Administrative Templates for Windows XP Professional and Windows Server 2003:


- For more information about the location of .adm files, see the Microsoft Knowledge Base article "Location of ADM (Administrative Template) Files in Windows" at http://support.microsoft.com/?scid=228460.

- For more information about how to create custom administrative template files in Windows, see the Microsoft Knowledge Base article “How to: Create Custom Administrative Templates in Windows 2000” at http://support.microsoft.com/?scid=323639.

- For information about how to create your own Administrative Templates, see the white paper "Implementing Registry–Based Group Policy" at www.microsoft.com/windows2000/techinfo/howitworks/management/rbppaper.asp.

- For information about error reporting, see the Windows Corporate Error Reporting Web site at www.microsoft.com/resources/satech/ cer/.


- For more information about Group Policy Management, see Enterprise Management with the Group Policy Management Console at www.microsoft.com/windowsserver2003/gpmc/.


- The "Office 2003 Policy Template Files and Deployment Planning Tools" download includes the Office Group Policy Administrative Template files and spreadsheets that summarize all of the available settings at http://download.microsoft.com/download/9/5/f/95f7e000-d7ab-4b86-8a5d-804b124c7a69/Office-2003-SP1-ADMs-OPAs-and-Explain-Text.exe.

- The "Office 2003 Resource Kit toolset" includes the "Office 2003 Policy Template Files and Deployment Planning Tools" as well as a number of other useful tools for deploying and managing Office 2003 at http://download.microsoft.com/download/0/e/d/0eda9ae6-f5c9-44be-98c7-ccc3016a296a/ork.exe.
• The two-part MSDN article “Browsing the Web and Reading E-mail Safely as an Administrator” explains how you can configure Web browsers and mail clients to execute at lower privileges when you log on to your computer with an account that has administrator privileges. The two parts are available online at

Additional Registry Entries

This chapter provides additional information about registry entries (also called registry values) for the baseline security template file that are not defined within the Administrative Template (.adm) file. The .adm file defines the policies and restrictions for the desktop, shell, and security for Microsoft® Windows Server™ 2003.

Customized Security Configuration Editor

When you load the Microsoft Management Console (MMC) Security Templates snap-in and view the security templates, the entries in the following tables are not represented. These entries were added to the .inf file by using a customized version of the Security Configuration Editor (SCE). These entries can also be viewed or modified with a text editor such as Notepad. They will be applied to computers when policies are downloaded to them, regardless of whether the computers have also had their SCE user interfaces modified.

These entries are embedded within the security templates to automate the changes. If the policy is removed, these entries are not automatically removed with it; they must be manually changed using a registry editing tool such as Regedt32.exe. The Microsoft Excel® workbook "Windows Default Security and Services Configuration" that is included with this guide documents the default settings.

How to Modify the Security Configuration Editor User Interface

The SCE is used to define security templates that can be applied to individual computers or any number of computers through Group Policy. Security templates can contain password policies, lockout policies, Kerberos protocol policies, Audit policies, event log settings, registry values, service startup modes, service permissions, user rights, group membership restrictions, registry permissions, and file system permissions. The SCE appears in a number of MMC snap-ins and administrator tools. It is used by the Security Templates snap-in and the Security Configuration and Analysis snap-in. The Group Policy Editor snap-in uses it for the Security Settings portion of the Computer Configuration tree. It is also used for the Local Security Settings, Domain Controller Security Policy, and the Domain Security Policy tools as well.
This guide includes additional entries that are added to the SCE by modifying the Seregvl.inf file (located in the %systemroot%\inf folder) and re-registering the Scecli.dll file. The original security settings, as well as the additional ones, appear under Local Policies\Security in the snap-ins and tools listed earlier in this guide. You should update the Seregvl.inf file and re-register the Scecli.dll file on any computers for which you will edit the security templates and Group Policies that are provided with this guide as described in the following sections. However, the customization information for the Seregvl.inf file uses features that only became available in Microsoft Windows® XP Professional with Service Pack 1 (SP1) and Windows Server 2003—do not try to install it on older versions of Windows.

After the Seregvl.inf file has been modified and registered, the custom registry values are exposed in the SCE user interfaces on that computer. You will see the new settings at the bottom of the list of items in the SCE; the new settings all have names that start with "MSS:" MSS stands for Microsoft Solutions for Security, the name of the group that created this guide. You can then create security templates or policies that define these new registry values. These templates or policies can then be applied to any computer regardless of whether Seregvl.inf has been modified on the target computer or not. Subsequent launches of the SCE UI will expose your custom registry values.

Instructions about how to modify the SCE user interface are provided in the following procedures. There are manual instructions that you should follow if you have already made other customizations to the SCE. A script is provided to add the settings with minimal user interaction, and although the script has error detection and recovery features built in, it may fail. If it fails, you should determine the cause of the failure and either correct the problem or follow the manual instructions. Another script is provided that you can use to restore the SCE user interface to its default state. This script will remove all custom settings and return the SCE to the way it appears in a default installation of Windows XP with SP2 or Windows Server 2003 with SP1.

To manually update Seregvl.inf

1. Use a text editor such as Notepad to open the Values-seregvl.txt file from the SCE Update folder of the download for this guide.
2. Open another window in the text editor and then open the %systemroot%\inf\seregvl.inf file.
3. Navigate to the bottom of the "[Register Registry Values]" section in the seregvl.inf file. Copy and paste the text from the Values-seregvl.txt file, without any page breaks, into this section of the seregvl.inf file.
4. Close the Values-seregvl.txt file and open the Strings-seregvl.txt file from the SCE Update folder of the download.
5. Navigate to the bottom of the "[Strings]" section in the seregvl.inf file. Copy and paste the text from the Strings-seregvl.txt file, without any page breaks, into this section of the seregvl.inf file.
6. Save the seregvl.inf file and close the text editor.
7. Open a command prompt and execute the command regsvr32 scecli.dll to re-register the DLL file.

Subsequent launches of the SCE will display these custom registry values.
To automatically update sceregvl.inf

1. The Values-sceregvl.txt, Strings-sceregvl.txt, and Update_SCE_with_MSS_Regkeys.vbs files that are located in the SCE Update folder of the download for this guide must all be in the same location for the script to function.
2. Execute the Update_SCE_with_MSS_Regkeys.vbs script on the computer you wish to update.
3. Follow the onscreen prompts

This procedure will remove only the custom entries made using the script that is described in the previous procedure, Update_SCE_with_MSS_Regkeys.vbs. You can also reverse the changes made by the automatic update script.

To reverse the changes made by the Update_SCE_with_MSS_Regkeys.vbs script

1. Execute the Rollback_SCE_for_MSS_Regkeys.vbs script on the computer you wish to update.
2. Follow the onscreen prompts

This procedure will remove any custom entries that you may have added to the SCE user interface, including those from this guide and others that may have been provided in earlier versions of this guide or in other security guides.

To restore the SCE to its default state for Windows XP with SP2 and Windows Server 2003 with SP1

1. The sceregvl_W2K3_SP1.inf.txt, sceregvl_XPSP2.inf.txt, and Restore_SCE_to_Default.vbs files that are located in the SCE Update folder of the download for this guide must all be in the same location for the script to function.
2. Execute the Restore_SCE_to_Default.vbs script on the computer you wish to update.
3. Follow the onscreen prompts

To manually restore the SCE user interface to its default appearance

1. Click Start, Run, type regedit.exe and press ENTER to open the Registry Editor tool.
2. Navigate to HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\SecEdit\Reg Values.
3. Each subkey in this location represents one item in the Security Options section of the SCE. Carefully delete all of the subkeys. Do not delete the parent key (Reg Values), but only the subkeys that are contained within it.
4. Open a command prompt and execute the command regsvr32 scecli.dll to re-register the SCE DLL.
5. Subsequent launches of the SCE will only display the original registry values that were included with your version of Windows.
TCP/IP-Related Registry Entries

To help prevent denial of service (DoS) attacks, you should keep your computer updated with the latest security fixes and harden the TCP/IP protocol stack on your Windows Server 2003 computers that are exposed to potential attackers. The default TCP/IP stack configuration is tuned to handle standard intranet traffic. If you connect a computer directly to the Internet, Microsoft recommends that you harden the TCP/IP stack to protect against DoS attacks.

DoS attacks that are directed at the TCP/IP stack tend to be of two classes: attacks that use an excessive number of system resources (one way to do this is to open numerous TCP connections) or attacks that send specially crafted packets that cause the network stack or the entire operating system to fail. The following registry settings help to protect against the attacks that are directed at the TCP/IP stack.

The registry settings in the following table were added to the template file in the \HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\ subkey. More detailed information about each of the settings is provided in the subsections that follow the table and on the Microsoft Windows Server 2003 TCP/IP Implementation Details page at www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/networking/tcpip03.mspx.

Table 10.1 TCP/IP-Related Registry Entries in Windows Server 2003 with SP1 and Windows XP with SP2

<table>
<thead>
<tr>
<th>Registry entry</th>
<th>Format</th>
<th>XP SP2 default</th>
<th>2003 SP1 default</th>
<th>Most secure value (decimal)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DisableIPSourceRouting</td>
<td>DWORD</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>EnableDeadGWDetect</td>
<td>DWORD</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>EnableICMPRedirect</td>
<td>DWORD</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>KeepAliveTime</td>
<td>DWORD</td>
<td>7200000</td>
<td>7200000</td>
<td>300,000</td>
</tr>
<tr>
<td>PerformRouterDiscovery</td>
<td>DWORD</td>
<td>2</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>SynAttackProtect</td>
<td>DWORD</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>TcpMaxConnectResponseRetransmissions</td>
<td>DWORD</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>TcpMaxDataRetransmissions</td>
<td>DWORD</td>
<td>5</td>
<td>5</td>
<td>3</td>
</tr>
</tbody>
</table>

_DisableIPSourceRouting:_ **IP source routing protection level (protects against packet spoofing)**

This 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 follow through the network.
Chapter 10: Additional Registry Entries

Vulnerability
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.

Countermeasure
Configure the MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing) entry to a value of Highest protection, source routing is completely disabled.

The possible values for this registry entry are:
• 0, 1, or 2. The default configuration is 1 (source routed packets are not forwarded).

In the SCE UI, the following list of options appears:
• No additional protection, source routed packets are allowed.
• Medium, source routed packets ignored when IP forwarding is enabled.
• Highest protection, source routing is completely disabled.
• Not Defined.

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

EnableDeadGWDetect: Allow automatic detection of dead network gateways (could lead to DoS)

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.

Vulnerability
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.

Countermeasure
Configure the MSS: (EnableDeadGWDetect) Allow automatic detection of dead network gateways (could lead to DoS) entry to a value of Disabled.

The possible values for this registry entry are:
• 1 or 0. The default configuration is 1 (enabled) on Windows Server 2003.

In the SCE UI, these options appear as:
• Enabled
• Disabled
• Not Defined
Potential Impact
If you configure this value to 0, Windows cannot detect dead gateways and automatically switch to alternates.

**EnableICMPRedirect: Allow ICMP redirects to override OSPF generated routes**

This 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.

Vulnerability
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.

Countermeasure
Configure the **MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes** entry to a value of Disabled.

The possible values for this registry entry are:

- 1 or 0. The default configuration is 1 (enabled).

In the SCE UI, these options appear as:

- Enabled
- Disabled
- Not Defined

Potential 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.

**KeepAliveTime: How often keep-alive packets are sent in milliseconds (300,000 is recommended)**

This entry appears as **MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds (300,000 is recommended)** in the SCE. It controls how often TCP sends a keep-alive packet to verify that an idle connection is still intact. If the remote computer is still reachable, it acknowledges the keep-alive packet.
Vulnerability
An attacker who is able to connect to network applications could establish numerous connections to cause a DoS condition.

Countermeasure
Configure the MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds (300,000 is recommended) entry to a value of 300000 or 5 minutes.

The possible values for this registry entry are:
• 1 through 0xFFFFFFFF. The default configuration is 7,200,000 (two hours).

In the SCE UI, the following list of options appears:
• 150000 or 2.5 minutes
• 300000 or 5 minutes (recommended)
• 600000 or 10 minutes
• 1200000 or 20 minutes
• 2400000 or 40 minutes
• 3600000 or 1 hour
• 7200000 or 2 hours (default value)
• Not Defined

Potential 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.

PerformRouterDiscovery: Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)

This entry appears as MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS) in the SCE. It enables or disables the Internet Router Discovery Protocol (IRDP). IRDP allows the computer to detect and configure default gateway addresses automatically (as described in RFC 1256) on a per-interface basis.

Vulnerability
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.

Countermeasure
Configure the MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS) entry to a value of Disabled.
The possible values for this registry entry are:
- 0, 1, or 2. The default configuration is 2 (enable only if DHCP sends the Perform Router Discovery option).

In the SCE UI, these options appear as:
- 0 (Disabled)
- 1 (Enabled)
- 2 (enable only if DHCP sends the Perform Router Discovery option)
- Not Defined

**Potential Impact**

If you disable this entry, Windows Server 2003 (which supports the IRDP) cannot automatically detect and configure default gateway addresses on the computer.

**SynAttackProtect: Syn attack protection level (protects against DoS)**

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).

**Vulnerability**

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.

**Countermeasure**

Configure the MSS: (SynAttackProtect) Syn attack protection level (protects against DoS) entry to a value of Connections time out sooner if a SYN attack is detected.

The possible values for this registry entry are:
- 1 or 0. The default configuration is 1 (enabled) for Windows Server 2003 SP1 and 0 (disabled) for Windows XP SP2.

In the SCE UI, these options appear as:
- Connections time out more quickly if a SYN attack is detected
- No additional protection, use default settings
- Not Defined

**Potential 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.

**TcpMaxConnectResponseRetransmissions:** SYN-ACK retransmissions when a connection request is not acknowledged

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.

**Vulnerability**

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.

**Countermeasure**

Configure the MSS: (TcpMaxConnectResponseRetransmissions) SYN-ACK retransmissions when a connection request is not acknowledged entry to a value of 3 seconds, half-open connections dropped after nine seconds.

The possible values for this registry entry are:

- 0-0xFFFFFFFF. The default configuration is 2.
- 3, 6, & 9 seconds, half-open connections dropped after 45 seconds
- Not Defined

**Potential 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.
**TcpMaxDataRetransmissions: How many times unacknowledged data is retransmitted (3 recommended, 5 is default)**

This entry appears as MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default) in the SCE. This entry controls the number of times that TCP retransmits an individual data segment (non-connect segment) before it aborts the connection. 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.

**Vulnerability**

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.

**Countermeasure**

Configure the MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default) entry to a value of 3. The possible values for this registry entry are:

- 0 to 0xFFFFFFFF. The default configuration is 5.

In the SCE UI, this setting can be adjusted using a text entry box:

- A user-defined number
- Not Defined

**Potential 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.
### Miscellaneous Registry Entries

The registry entries in the following table are also recommended. Additional information about each entry, including the location of each registry key setting, is provided in the subsections that follow the table.

**Table 10.2 Non-TCP/IP Entries Added to Registry in Windows Server 2003**

<table>
<thead>
<tr>
<th>Registry entry</th>
<th>Format</th>
<th>Most secure value (decimal)</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)</td>
<td>DWORD</td>
<td>Not defined, except for highly secure environments, which should use 0.</td>
</tr>
<tr>
<td>MSS: (AutoReboot) Allow Windows to automatically restart after a system crash (recommended except for highly secure environments)</td>
<td>DWORD</td>
<td>Not defined, except for highly secure environments, which should use 0.</td>
</tr>
<tr>
<td>MSS: (AutoShareWks) Enable Administrative Shares (not recommended except for highly secure environments)</td>
<td>DWORD</td>
<td>Not defined, except for highly secure environments, which should use 1.</td>
</tr>
<tr>
<td>MSS: (DisableSavePassword) Prevent the dial-up password from being saved (recommended)</td>
<td>DWORD</td>
<td>1</td>
</tr>
<tr>
<td>MSS: (Hidden) Hide Computer From the Browse List (not recommended except for highly secure environments)</td>
<td>DWORD</td>
<td>Not defined, except for highly secure environments, which should use 1.</td>
</tr>
<tr>
<td>MSS: (NoDefaultExempt) Enable NoDefaultExempt for IPSec Filtering (recommended)</td>
<td>DWORD</td>
<td>1 for computers that run Windows XP, 3 for computers that run Windows Server 2003.</td>
</tr>
<tr>
<td>MSS: (NoDriveTypeAutoRun) Disable Autorun for all drives (recommended)</td>
<td>DWORD</td>
<td>0xFF</td>
</tr>
<tr>
<td>MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers (Only recommended for servers)</td>
<td>DWORD</td>
<td>1</td>
</tr>
<tr>
<td>MSS: (NtfsDisable8dot3NameCreation) Enable the computer to stop generating 8.3 style filenames (recommended)</td>
<td>DWORD</td>
<td>1</td>
</tr>
<tr>
<td>MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)</td>
<td>DWORD</td>
<td>1</td>
</tr>
<tr>
<td>MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)</td>
<td>String</td>
<td>0</td>
</tr>
</tbody>
</table>
### Registry entry

<table>
<thead>
<tr>
<th>MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning</th>
</tr>
</thead>
<tbody>
<tr>
<td>DWORD</td>
</tr>
<tr>
<td>0</td>
</tr>
</tbody>
</table>

### Disable Automatic Logon: Disable Automatic Logon

This entry appears as **MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)** in the SCE. This entry determines whether the automatic logon feature is enabled. (This entry is separate from the Welcome screen feature in Windows XP; if you disable that feature, this entry is not affected.) By default, this entry is not enabled. Automatic logon uses the domain, user name, and password that is stored in the registry to log users on to the computer when the computer starts. The log on dialog box is not displayed.

For additional information, see the Microsoft Knowledge Base article "How to turn on automatic logon in Windows XP" at http://support.microsoft.com/default.aspx?kbid=315231.

You can add this registry value to the template file in the

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\...
```

**Vulnerability**

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.

### Countermeasure

Do not configure the **MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)** entry except on highly secure computers, where it should be configured to a value of **Disabled**.

The possible values for this registry entry are:

- 1 or 0. The default configuration is 0 (disabled).

In the SCE UI, these options appear as:

- Enabled
- Disabled
- Not Defined
Potential Impact
None. By default this entry is not enabled.

Configure Automatic Reboot from System Crashes
This entry appears as MSS: (AutoReboot) Allow Windows to automatically restart after a system crash (recommended except for highly secure environments) in the SCE. It determines whether the computer restarts automatically after it fails.

You can add this registry value to the template file in the

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl\`
```

subkey.

Vulnerability
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.

Countermeasure
Configure the MSS: (AutoReboot) Allow Windows to automatically restart after a system crash (recommended except for highly secure environments) entry to a value of Disabled.

The possible values for this registry entry are:
• 1 or 0. The default configuration is 1 (enabled).

For more information, see the Microsoft Knowledge Base article "How To Configure System Failure and Recovery Options in Windows" at http://support.microsoft.com/?kbid=307973.

In the SCE UI, the following options are available:
• Enabled
• Disabled
• Not Defined

Potential Impact
The computer will no longer reboot automatically after a failure.

Enable Administrative Shares
This entry appears as MSS: (AutoShareWks) Enable Administrative Shares (not recommended except for highly secure environments) in the SCE. By default, Windows XP Professional automatically creates administrative shares such as C$ and IPC$.

For additional information, see the Microsoft Knowledge Base article "How to create and delete hidden or administrative shares on client computers" at http://support.microsoft.com/default.aspx?kbid=314984.
You can add this registry value to the template file in the

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters\subkey.

**Vulnerability**

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.

**Countermeasure**

Do not configure the **MSS: (AutoShareWks) Enable Administrative Shares (not recommended except for highly secure environments)** entry except on highly secure computers, where it should be configured to a value of **Enabled**.

The possible values for this registry entry are:

- 1 or 0. The default configuration is 1 (enabled).

In the SCE UI, these options appear as:

- Enabled
- Disabled
- Not Defined

**Potential 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 2000 require administrative shares for correct installation and operation. Also, many third-party network backup applications require administrative shares.

**Disable Saving of Dial-Up Passwords**

This entry appears as **MSS: (DisableSavePassword) Prevent the dial-up passsword from being saved (recommended)** in the SCE. It determines whether the passwords that are associated with Network Connections phone book entries are saved. If the user has many phone book entries, accumulated saved passwords can cause a slight delay after the user's credentials are entered in the **Connecting To** dialog box.

You can add this registry value to the template in the

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Parameters\subkey.

**Vulnerability**

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.
Countermeasure

Configure the **MSS: (DisableSavePassword)** Prevent the dial-up password from being saved (recommended) entry to a value of **Disabled**.

The possible values for this registry entry are:

- 1 or 0. The default configuration is 0 (disabled).

For more information, see the Microsoft Knowledge Base article "Disabling Save Password Option in Dial-Up Networking" at http://support.microsoft.com/default.aspx?kbid=172430.

In the SCE UI, the following options are available:

- Enabled
- Disabled
- Not Defined

Potential Impact

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

**Hide the Computer from Network Neighborhood Browse Lists: Hide Computer From the Browse List**

This 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, you hide the computer from the Browser list; it does not announce itself to other computers on the same network.

For more information, see the Microsoft Knowledge Base article "HOW TO: Hide a Windows 2000–Based Computer from the Browser List" at http://support.microsoft.com/default.aspx?kbid=321710.

You can add this registry value to the template file in the

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Lanmanserver\Parameters\
```

subkey.

Vulnerability

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.

Countermeasure

Do not configure the **MSS: (Hidden) Hide Computer From the Browse List** (not recommended except for highly secure environments) entry except on highly secure computers, where it should be configured to a value of **Enabled**.
The possible values for this registry entry are:

- 1 or 0. The default configuration is 0 (disabled).

In the SCE UI, these options appear as:

- Enabled
- Disabled
- Not Defined

**Potential Impact**

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

**Enable IPSec to protect Kerberos RSVP Traffic: Enable NoDefaultExempt for IPSec Filtering**

This entry appears as **MSS: (NoDefaultExempt) Enable NoDefaultExempt for IPSec Filtering (recommended)** in the SCE. The default exemptions to IPsec policy filters are documented in the Microsoft Windows Server 2003 and Microsoft Windows XP online help. 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.

For more information, see the TechNet article “**Specifying Default Exemptions to IPSec Filtering**” at www.microsoft.com/technet/prodtechnol/windowsserver2003/library/DepKit/c9a7d986-5b9a-4e01-bb80-82d5e3a87d5c.mspx. Also, see 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.

You can add this registry value to the template file in the

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\IPSEC\subkey.
```

**Vulnerability**

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.

**Countermeasure**

Do not configure the **MSS: (NoDefaultExempt) Enable NoDefaultExempt for IPSec Filtering (recommended)** entry except on computers that use IPsec filters, where this entry should be configured to a value of **Enabled**.
The possible values for this registry entry are:

- A value of 0 specifies that multicast, broadcast, RSVP, Kerberos, and IKE (ISAKMP) traffic are exempt from IPsec filters, which is the default configuration for Windows 2000 and Windows XP. Use this setting only if you require compatibility with an IPsec policy that already exists or Windows 2000 and Windows XP.

- A value of 1 specifies that Kerberos protocol and RSVP traffic are not exempt from IPsec filters, but multicast, broadcast, and IKE traffic are exempt. This setting is the recommended value for Windows 2000 and Windows XP.

- A value of 2 specifies that multicast and broadcast traffic are not exempt from IPsec filters, but RSVP, Kerberos, and IKE traffic are exempt. This setting is supported only in Windows Server 2003.

- A value of 3 specifies that only IKE traffic is exempt from IPsec filters. This setting is supported only in Windows Server 2003, which contains this default behavior although the registry key does not exist by default.

In the SCE UI, these options appear as:
- 0
- 1
- 2
- 3

**Potential 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, which was referenced earlier in this section.

**Disable Autorun: Disable Autorun for all drives**

This entry appears as **MSS: (NoDriveTypeAutoRun) Disable Autorun for all drives (recommended)** in the SCE. Autorun starts to read from a drive on your computer as soon as media is inserted in it. As a result, the setup file of programs and the sound on audio media starts immediately.

To disable Autorun in all drives, you can add this registry value to the template file in the

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\
```

subkey.

Alternatively, to disable Autorun for CD/DVD drives only, you can add this registry value to the template file in the

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Cdrom\
```

subkey.
Vulnerability
To prevent a possible malicious program from execution when media is inserted, the Group Policy disables Autorun on all drives.

An attacker with physical access to the computer could insert an Autorun-enabled DVD or CD into the computer that will automatically launch a malicious program.

Countermeasure
Configure the MSS: (NoDriveTypeAutoRun) Disable Autorun for all drives (recommended) entry to a value of 255, disable Autorun for all drives.

The possible values for this registry entry are:

• A range of hexadecimal values

For more information, see Microsoft Knowledge Base article "The AutoRun feature or the AutoPlay feature does not work when you insert a CD-ROM in the drive" at http://support.microsoft.com/default.aspx?kbid=330135.

In the SCE UI, the following options are available:

• Null, allow Autorun
• 255, disable Autorun for all drives
• Not Defined

Potential Impact
Autorun will no longer work when Autorun-enabled discs are inserted into the computer. Also, CD-burning utilities may not work as expected because blank CDs may not be recognized. Media applications such as Windows Media Player will not recognize new CDs or DVDs that are inserted, which will force users to manually launch them.

Configure NetBIOS Name Release Security:
(NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers

This entry appears as MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers (Only recommended for servers) in the SCE. NetBIOS over TCP/IP (NetBT) is a networking protocol that, among other things, provides a way to easily resolve NetBIOS names that are registered on Windows–based computers to the IP addresses that are configured on those computers. This value determines whether the computer releases its NetBIOS name when it receives a name-release request.

You can add this registry value to the template file in the

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netbt\Parameters\ subkey.
Vulnerability

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.

Countermeasure

Configure the MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers (Only recommended for servers) entry to a value of Enabled.

The possible values for this registry entry are:

- 1 or 0. The default configuration is 1 (enabled).

In the SCE UI, these options appear as:

- Enabled
- Disabled
- Not Defined

Alternatively, you could disable the use of WINS in your environment, and further ensure that all applications rely upon DNS for name resolution services. Although this approach is a recommended long-term strategy, it is generally impractical for most organizations to attempt as a short-term solution. Organizations that still run WINS generally have application dependencies that cannot be quickly resolved without upgrades and software rollouts, which require careful plans and significant time commitments.

If you cannot deploy this countermeasure and you want to guarantee NetBIOS name resolution, you can take the additional step of "pre-loading" NetBIOS names in the LMHOSTS file on certain computers. For more information about how to pre-load the LMHOSTS file, see the Microsoft Knowledge Base article "MS00-047: NetBIOS Vulnerability May Cause Duplicate Name on the Network Conflicts" that was referenced earlier in this section.

Note: Maintenance of LMHOSTS files in most environments requires a significant amount of effort. Microsoft encourages the use of WINS instead of LMHOSTS.

Potential 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, Microsoft recommends that you test this change in a non-production environment before you change the production environment.
**Disable Auto Generation of 8.3 File Names: Enable the computer to stop generating 8.3 style filenames**

This entry appears as `MSS: (NtfsDisable8dot3NameCreation) Enable the computer to stop generating 8.3 style filenames (recommended)` in the SCE.

Windows Server 2003 supports 8.3 file name formats for backward compatibility with 16-bit applications. (The 8.3 file name convention is a naming format that allows file names that are up to eight characters in length.)

You can add this registry value to the template file in the

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem\[subkey].
```

**Vulnerability**

If you allow 8.3 style file names, an attacker only needs eight characters to refer to a file that may be 20 characters long. For example, a file named `Thisisalongfilename.doc` could be referenced by its 8.3 filename, `Thisis~1.doc`. If you do not use 16-bit applications, you can turn this feature off. Also, directory enumeration performance is improved if you disable short name generation on an NTFS file system (NTFS) partition.

Attackers could use short file names to access data files and applications with long file names that would normally be difficult to locate. An attacker who has gained access to the file system could access data or execute applications.

**Countermeasure**

Configure the `MSS: (NtfsDisable8dot3NameCreation) Enable the computer to stop generating 8.3 style filenames (recommended)` entry to a value of Enabled.

The possible values for this registry entry are:

- 1 or 0. The default configuration is 0 (disabled).

In the SCE UI, these options appear as:

- Enabled
- Disabled
- Not Defined

**Potential Impact**

The 16-bit applications in your organization will not be able to access files that are not named with the 8.3 format. Some 32-bit applications also rely on the presence of short names, because short names tend not to contain embedded spaces and therefore do not require quotation marks when used in command lines. The installation routines for some programs may fail; those that are designed to run on multiple CPU architectures are likely to be 16-bit applications. The installation of Exchange 2000 SP2 will fail if this entry is enabled. The installation of service packs for SQL 2000 will fail if this entry is enabled and the path for the system variable `%temp%` includes a space; a simple workaround for this problem is to redefine the variable to a path without spaces (for example, `C:\temp`).

**Note:** If you apply this entry to a server that already has files with auto-generated 8.3 file names, it does not remove them. To remove existing 8.3 file names, you will need to copy those files off the server, delete the files from the original location, and then copy the files back to their original locations.
Enable Safe DLL Search Order: Enable Safe DLL search mode (recommended)

This entry appears as MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended) in the SCE. The dynamic-link library (DLL) search order can be configured to search for requested DLLs in one of two ways:

If SafeDllSearchMode is configured to 1, the search order is as follows:

- The directory from which the application loaded.
- The system directory.
- The 16-bit system directory. There is no function that obtains the path of this directory, but it is searched.
- The Windows directory.
- The current directory.
- The directories that are listed in the PATH environment variable.

If SafeDllSearchMode is configured to 0, the search order is as follows:

- The directory from which the application loaded.
- The current directory.
- The system directory.
- The 16-bit system directory. There is no function that obtains the path of this directory, but it is searched.
- The Windows directory.
- The directories that are listed in the PATH environment variable.

You can add this registry value the template file in the

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

subkey.

Vulnerability

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.

Countermeasure

Configure the MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended) entry to a value of Enabled.

The possible values for this registry entry are:

- 1 or 0. The default configuration for Windows XP is 0 and it is 1 for Windows Server 2003.

In the SCE UI, these options appear as:

- Enabled
- Disabled
- Not Defined
Potential 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.

**Make Screensaver Password Protection Immediate: The time in seconds before the screen saver grace period expires (0 recommended)**

This 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 if screen saver locking is enabled.

You can add this registry value to the template file in the

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

subkey.

Vulnerability

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.

Countermeasure

Configure the MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended) entry to a value of 0.

The possible values for this registry entry are:

- 0 to 255. The default value is 5 seconds.

In the SCE UI, the value for this entry appears as a text entry box:

- A user-defined number
- Not Defined

Potential Impact

Users will have to enter their passwords to resume their console sessions as soon as the screen saver activates.
Security Log Near Capacity Warning:
Percentage threshold for the security event log at which the system will generate a warning

This entry appears as MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning in the SCE. Windows Server 2003 and Service Pack 3 for Windows 2000 include a new feature to generate a security audit in the Security event log when it reaches a user-defined threshold. For example, if this value is set to 90, an event entry with eventID 523 will be entered in the log when the Security log reaches 90 percent of capacity. This entry contains the following text:

The security event log is 90 percent full.

Note: This setting will have no effect if the Security event Log is configured to overwrite events as needed.

You can add this registry value to the template file in the

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security\ subkey.

Vulnerability

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.

Countermeasure

Configure the MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning entry to a value of 90.

The possible values for this registry entry are:

• 0 to 100. The default configuration is 0 (no warning event is generated).

In the SCE UI, the following options are available:

• 50%
• 60%
• 70%
• 80%
• 90%
• Not Defined

Potential 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.
Registry Entries Available in Windows XP with SP2 and Windows Server 2003 with SP1

The registry entries that are described earlier in this chapter apply to Microsoft Windows XP with SP1 and Windows Server 2003.

The release of Windows XP SP2 and Windows Server 2003 SP1 provided additional security-related registry entries that you can configure to address specific security requirements in your environment.

The following registry entries are available in both Windows XP with SP2 and Windows Server 2003 with SP1.

**RestrictRemoteClients**

When an interface is registered through RpcServerRegisterIf, RPC allows the server application to restrict access to the interface, typically through a security callback. The **RestrictRemoteClients** registry key forces RPC to perform additional security checks for all interfaces, even if the interface has no registered security callback. RPC clients that use the named pipe protocol sequence (ncacn_np) are exempt from these restrictions. The named pipe protocol sequence cannot be restricted because of several significant backward-compatibility issues.

The **RestrictRemoteClients** registry key can have one of three DWORD values:

- **0.** This value is the default value in Windows Server 2003 with SP1, and it causes the computer to bypass the RPC interface restriction. It is entirely the responsibility of the server application to impose appropriate RPC restrictions. This configuration is equivalent to the configuration of previous versions of Windows.

- **1.** This value is the default value in Windows XP with SP2. All remote anonymous calls are rejected by the RPC runtime except calls that come in through named pipes (ncacn_np).

- **2.** All remote anonymous calls are rejected by the RPC runtime with no exemptions. In this configuration, a computer cannot receive remote anonymous calls using RPC.

Developers can modify their applications to pass flags to the RPC subsystem that indicate whether the client or server will accept anonymous RPC requests.

**Vulnerability**

RPC interfaces that allow unauthenticated connections can potentially be used to remotely exploit buffer overruns and spread malicious code.

**Countermeasure**

The default configuration of the **RestrictRemoteClients** value in both Windows Server 2003 with SP1 and Windows XP with SP2 allow backward compatibility. To add protection against worms that may attempt to remotely exploit buffer overflows in RPC services, configure **RestrictRemoteClients** to 1 or 2.
Potential Impact

If you enable the **RestrictRemoteClients** registry key, the RPC Endpoint Mapper interface will not be accessible anonymously. This restriction is a significant security improvement, but it changes how endpoints are resolved. Currently, an RPC client that attempts to make a call by using a dynamic endpoint will first query the RPC Endpoint Mapper on the server to determine what endpoint it should connect to. This query is performed anonymously, even if the RPC client call uses RPC security. Anonymous calls to the RPC Endpoint Mapper interface will fail on Windows Server 2003 with SP1 if the **RestrictRemoteClients** key is set to 1 or higher. Therefore, the RPC client runtime must be modified to perform an authenticated query to the Endpoint Mapper. If the **EnableAuthEpResolution** key is set, the RPC client runtime will use NTLM to authenticate to the Endpoint Mapper. This authenticated query will take place only if the actual RPC client call uses RPC authentication.

Some applications and services may not work properly when this key is enabled. Therefore you should test it thoroughly before you deploy it in your environment. If you plan to enable this key, you should also use the **EnableAuthEpResolution** key to enable authentication for the RPC Endpoint Mapper.

**EnableAuthEpResolution**

Anonymous calls to the RPC Endpoint Mapper interface will fail by default on Windows XP with SP2 because of the default value for the new **RestrictRemoteClients** key. Therefore, the RPC client runtime must be modified to perform an authenticated query to the Endpoint Mapper. To do so, configure the **EnableAuthEpResolution** key to 1. When this configuration is in place, the RPC client runtime will use NTLM to authenticate to the Endpoint Mapper interface. This authenticated query will only take place if the actual RPC client call uses RPC authentication.

**Vulnerability**

RPC interfaces that allow unauthenticated connections can potentially be used to remotely exploit buffer overruns and spread malicious code.

**Countermeasure**

To add protection against worms that may attempt to remotely exploit buffer overflows in RPC services, configure **RestrictRemoteClients** as described in the previous section and then use **EnableAuthEpResolution** to enable NTLM authentication for computer RPC requests.

**Potential Impact**

Clients that do not have the **EnableAuthEpResolution** key set will not be able to make RPC service requests of servers that have **RestrictRemoteClients** enabled. This restriction may cause RPC-based services to stop working.

**RunInvalidSignatures**

By default, Windows Server 2003 with SP1 and Windows XP with SP2 prevent the installation of signed code objects that have invalid signatures. These signatures may be invalid because the code has been modified, because the signing certificate has expired, or because the signing certificate appears on a certificate revocation list (CRL). Internet Explorer 6.0 already blocked the installation of signed code with invalid signatures, but the service pack extends this behavior to all applications.
Vulnerability
A signed Microsoft ActiveX® control that has been tampered with may be downloaded and run by an application, which could compromise the computer on which it runs.

Countermeasure
The default value of RunInvalidSignatures blocks this vulnerability.

Potential Impact
Applications that depend on legitimate signed controls will not function if those controls' signatures are invalid for any reason. If you have an application whose signature appears to be invalid, you can change this key configuration to allow the control to download and run. However, doing so creates a security vulnerability. The preferred solution is to contact the developers of the control that is used in the application to obtain a version with a valid signature.
Registry Entries Available in Windows XP with SP2

The following registry entries are available only in Windows XP with SP2.

Security Center Registry Entries for XP

There are three registry values for the Security Center that determine whether or not the user receives alerts for a given feature. If a key has a value of 0 or is nonexistent, the notification icon and alert system for that feature are enabled. If a value exists and is not 0, the notification icon and alert system for the feature is disabled.

All three of these values are located in HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Security Center. The values are:

- AntiVirusDisableNotify
- FirewallDisableNotify
- UpdatesDisableNotify

Vulnerability

Users who disable the alert features of Security Center may not receive appropriate warnings if the antivirus, firewall, or automatic update services that are installed on their computers do not work properly for some reason.

Countermeasure

Apply a Group Policy registry entry to enforce the appropriate warning configuration for your environment.

Potential Impact

These registry values are visible in the Security Center user interface if the Security Center functionality is enabled. Users with local administrator access will be able to change the Security Center values.

StorageDevicePolicies\WriteProtect

By default, users can mount USB block storage devices on their Windows XP computers and read from, or write to, these devices without limitation. In SP2, Microsoft added the ability for administrators to restrict the ability of users to write to USB block storage devices.

To restrict users' ability to write to these devices, you can add the WriteProtect DWORD value to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies and configure it to 1. When this value is configured, the Windows driver for USB block storage devices will reject write requests to mounted USB block storage devices.

Vulnerability

An attacker could copy data to a removable USB device and steal it.
Countermeasure

When the WriteProtect value is set to 1, Windows XP with SP2 will block writes to USB block storage devices.

Potential Impact

This registry key provides partial mitigation of a serious threat. However, there are many other ways that a skilled attacker can steal data with a USB device. For example, a USB device can be programmed to enumerate as a non-block storage device (like a printer or CD-ROM device), which will bypass this control. Organizations that wish to prevent the theft of sensitive data by users or attackers can use this entry as part of a broader security strategy, in conjunction with physical access controls and other measures to restrict access to writable USB devices.
Registry Entries Available in Windows Server 2003 with SP1

The following registry entries are available only in Windows Server 2003 with SP1.

**UseBasicAuth**

Distributed Authoring and Versioning (DAV) is an HTTP–based protocol that allows remote access to file systems and file servers. Users can use UNC paths to access resources on DAV servers. However, the WebDAV redirector in Windows Server 2003 communicates with Web servers that support DAV through HTTP; it cannot use SSL-protected HTTP sessions. When these Web sites allow the use of basic authentication, DAV requests will transmit the user's authentication credentials in plaintext.

In Windows Server 2003 with SP1, the WebDAV redirector has been modified so that it never sends user credentials with basic authentication. This modification may affect applications or business processes that depend on the computer's default DAV redirector. (Note that Microsoft Office uses its own independent DAV client and is not affected by this entry.)

Windows Server 2003 SP1 introduces the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WebClient\Parameters\UseBasicAuth subkey. If you configure its value to 1, the computer WebDAV redirector can communicate with Web servers that only support basic authentication.

**Vulnerability**

An attacker could set up a Web server that uses basic authentication, then trick or spoof users and make them attempt to connect to it to capture their credentials.

**Countermeasure**

By default, the Windows Server 2003 WebDAV redirector will not use basic authentication, which effectively blocks this vulnerability.

**Potential Impact**

Applications that use the built-in WebDAV redirector to access Web resources will fail if the Web server only supports basic authentication. To resolve this problem, you can either configure the Web server to support more secure authentication methods or enable the UseBasicAuth value. However, the preferred mechanism is to reconfigure the Web server, which does not allow exposure of users' credentials.

**DisableBasicOverClearChannel**

The WebDAV redirector is part of the remote file system stack. When users attempt to open URLs on remote computers, their credentials may be exposed if the remote server supports only basic authentication. An attacker may be able to spoof a user and direct them to a Web site that requests credentials (through DAV) and uses basic authentication. If the user responds, they would expose their credentials to the malicious host.
The **UseBasicAuth** registry entry controls whether basic authentication can be used for WebDAV requests. If you configure the `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WebClient\Parameters\DisableBasicOverClearChannel` value to 1, the use of basic authentication with other Web resources is blocked.

**Vulnerability**

An attacker could set up a Web server that uses basic authentication, then trick or spoof users and make them attempt to connect to it to capture their credentials.

**Countermeasure**

Configure the **DisableBasicOverClearChannel** value to 1 on client computers to restrict their ability to connect to HTTP servers by using basic authentication.

**Potential Impact**

Many embedded devices (such as routers, print servers, and copiers) that offer HTTP access only support basic authentication, as do some business applications. When **DisableBasicOverClearChannel** is configured to 1, client computers will not be able to authenticate to these devices or applications.
More Information

The following links provide additional information about some of the entries that are discussed in this chapter:


• For details about how to configure registry entries to disable Microsoft’s I/O device drivers, see the Microsoft Knowledge Base article “HOWTO: Use Group Policy to disable USB, CD-ROM, Floppy Disk and LS-120 drivers” at http://support.microsoft.com/default.aspx?kbid=555324.

• For more information about the architecture that underlies the creation, editing, and processing of security templates, see “How Security Settings Extension Works” at www.microsoft.com/technet/prodtechnol/windowsserver2003/library/TechRef/f546e58e-8473-4985-a05d-0b038dea4a9f.mspx. This article includes detailed information about Group Policy storage, precedence, and how some settings persist even when a particular Group Policy is no longer applied to a computer (often referred to colloquially as ‘tattooing’).

• For more information about how to customize the Security Configuration Editor user interface, see the Microsoft Knowledge Base article “How to Add Custom Registry Settings to Security Configuration Editor” at http://support.microsoft.com/?scid=214752.

• For more information about common network attack types, see “Common Types of Network Attacks,” extracted from the Windows 2000 Server Resource Kit, which is available online at www.microsoft.com/resources/documentation/Windows/2000/server/reskit/en-us/cnet/cndb_ips_ddui.asp.

• For more information about how to harden the Windows Server 2003 TCP/IP stack, see the Microsoft Knowledge Base article "How to Harden the TCP/IP Stack Against Denial of Service Attacks in Windows Server 2003” at http://support.microsoft.com/?scid=324270.
Additional Countermeasures

This chapter describes how to implement some additional countermeasures, such as securing accounts. This chapter also provides general background, references, and configuration guidance for using IP Security (IPsec) filters as an effective countermeasure against network attacks.

Member Server Hardening Procedures

Although you can apply most of the countermeasures that are discussed in this guide through Group Policy, there are additional settings that are difficult or impossible to apply through Group Policy. The following sections provide guidance about how to implement these additional settings for domain member servers.

Securing the Accounts

Microsoft® Windows Server™ 2003 with Service Pack 1 (SP1) has a number of built-in user accounts that cannot be deleted but can be renamed. Two of the most well-known built-in accounts in Windows Server 2003 are Guest and Administrator.

Vulnerability

By default, the Guest account is disabled on member servers and domain controllers. This configuration should not be changed. Many variations of malicious code use the built-in Administrator account in an initial attempt to compromise a server. You should rename the built-in Administrator account and alter its description to prevent compromise of remote servers by attackers who try to use this well-known account.

The value of this configuration change has diminished over the past few years since the release of attack tools that specify the security identifier (SID) of the built-in Administrator account to determine its true name and then break into the server. A SID is the value that uniquely identifies each user, group, computer account, and logon session on a network. It is not possible to change the SID of this built-in account.

Countermeasure

Rename the Administrator account and change the password to a long and complex value on every server.

Note: You can rename the built-in Administrator account through Group Policy. The baseline policies that are included with the Windows Server 2003 Security Guide do not implement this setting because every organization should choose a unique name for this account. To rename the
account, configure the **Rename administrator account** setting in Group Policy at the following location:

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security\Options
```

Ideally, organizations should employ different passwords on each server, although such a configuration requires significant management overhead. However, you should note that if your organization uses the same account names and passwords on all of the servers, an attacker who gains access to one member server will be able to gain access to all others. Record any changes that you make in a secure place.

**Potential Impact**

The users who manage the computers must keep track of what account name is assigned to each computer. Users who need to log in to a particular server with the local Administrator account will have to refer to this secured documentation to find out what the user name and password is for the server.

**NTFS**

The NTFS setting partitions support access control lists (ACLs) and, optionally, encryption—by means of the Encrypting File System (EFS)—at the file and folder levels. This support is not available with the file allocation table (FAT), FAT32, or FAT32x file systems. FAT32 is a version of the FAT file system that has been updated to permit significantly smaller default cluster sizes and support hard disks of up to two terabytes in size. FAT32 is included in Microsoft Windows® 95 OSR2, Windows 98, Windows Me, Windows Server 2003, and Windows XP.

**Vulnerability**

Files that you cannot protect with ACLs can be easily viewed, changed or deleted by unauthorized users who can access them locally or over the network. Other files can be protected with ACLs, but encryption provides much more protection and is a viable option for files that only need to be accessible to a single user.

**Countermeasure**

Format all partitions on every server with NTFS. Use the convert utility to non-destructively convert FAT partitions to NTFS, but remember that the utility configures the ACLs for the converted drive to Everyone: Full Control.

For Windows Server 2003 and Windows XP–based computers, apply the following security templates locally to configure the default file system ACLs:

- **For workstations.** `%windir%\inf\defltwk.inf`
- **For servers.** `%windir%\inf\defltsv.inf`
- **For domain controllers.** `%windir%\inf\defltdc.inf`


**Note:** The default domain controller security settings are applied when a server is promoted to a domain controller.

**Potential Impact**

There is no negative impact.
Important: Proper configuration of NTFS permissions will help protect your organization’s data from exposure or unauthorized modifications, but it is critical that you do not forget about physical security. An attacker who has gained physical control of a computer can boot it to an alternate operating system with a bootable CD-ROM or floppy disk. An attacker who has removed a hard disk from one of your organization’s computers can move it to a different, unmanaged computer. After the attacker has complete physical control of the storage media, it is very difficult to keep that data secure.

This fundamental problem of computer security also exists for the file systems of other operating systems. After an attacker has physical access to the disk, the NTFS permissions—and most other safeguards—can be easily bypassed. Obvious physical security measures your organization can implement include restricted access to buildings, installation of magnetic locks on server rooms, use of locks in server racks, and use of docking station locks for laptop computers. In addition to these security measures, Microsoft recommends the following additional technologies that can help lessen the impact of these types of attacks:

- Use Syskey with an offline password to prevent startup of the Windows operating system by unauthorized persons.
- Use EFS to encrypt user data. Instruct users to use their domain accounts and either configure no recovery agent or configure it for domain administrator accounts rather than the local administrator account.
- Use BIOS passwords to deny unauthorized users the ability to start computers within your organization.
- Configure the system BIOS to disable the ability of computers to start from CD-ROM drives and floppy disk drives. This configuration will deny the ability of unauthorized users to start computers with their own operating system.

Data and Application Segmentation

It has long been considered a best practice to locate data, applications, and operating system files on separate storage devices to improve computer performance. If you segregate these types of files on servers you also help protect the applications, data, and operating systems from directory traversal attacks.

Vulnerability

Two types of vulnerabilities are exposed if you locate applications, data, and log files on the same storage volume as the operating system. One vulnerability is the potential for a user or users to accidentally or deliberately fill an application log file or upload files to the server and fill the storage volume with data.

The second vulnerability is known as a directory traversal exploit, in which an attacker takes advantage of a bug in a network service to navigate the directory tree to the root of the system volume. The attacker may then search through the operating system file folders to execute a utility remotely.

There are thousands of variations on directory traversal attacks that exploit vulnerable applications and operating systems. IIS has been vulnerable to several such attacks in recent years. For example, the NIMDA and Code Red worms used a buffer overflow exploit to traverse Web site directory trees and then remotely execute Cmd.exe to gain access to a remote shell and execute additional commands.

Countermeasure

Whenever possible, relocate Web content, applications, data, and application log files to a partition that is separate from the system volume.
Potential Impact

For organizations that build and maintain servers in a consistent manner, the impact should be minimal. For organizations that do not maintain this information, the impact will be somewhat greater because administrators will have to investigate how each computer is set up.

**Configure SNMP Community Name**

The Simple Network Management Protocol (SNMP) is a network management standard that is widely used in TCP/IP networks. SNMP provides a way to manage network nodes—servers, workstations, routers, bridges, and hubs—from a centrally located host. SNMP performs its management services through a distributed architecture of management systems and agents. Computers that run network management software are referred to as SNMP management systems or SNMP managers. Managed network nodes are referred to as SNMP agents.

The SNMP service provides a rudimentary form of security by means of community names and authentication traps. You can restrict SNMP communications for agents and allow them to communicate with only a specific list of SNMP management systems, and community names can be used to authenticate SNMP messages. Although a host can belong to several communities at the same time, an SNMP agent does not accept requests from a management system in a community that is not on its list of acceptable community names. There is no relationship between community names and domain or workgroup names. A community name can be thought of as a password that is shared by SNMP management consoles and managed computers. It is your responsibility as a system administrator to create hard-to-guess community names when you install the SNMP service.

**Vulnerability**

The SNMP protocol is inherently weak with regard to security. The single biggest vulnerability with SNMP is that almost all vendors set a default community string name, and these default community names are well known. For example, Microsoft uses the word Public.

A second vulnerability is more difficult to overcome. Because SNMP traffic is sent in plaintext, the community string is transmitted across the network without being encrypted or hashed when an SNMP management device connects to an SNMP client. To address this second vulnerability, you can encrypt all traffic between servers. However, this countermeasure is beyond the scope of this guide.

**Countermeasure**

Configure the SNMP community string for read access on all computers to a random alphanumeric value.

**To configure the SNMP community string**

1. At the Services console, double-click SNMP Service.
2. Click the Security tab on the SNMP Service Properties dialog box.
3. Select public from the Accepted community names list.
4. Click the Edit button, and then type the new community name in the SNMP Service Community Name dialog box when it appears.
5. Click the OK button to close each of the dialog boxes.
Leave write access through SNMP disabled.

**Note:** The community name is stored in the registry as a registry value with a DWORD value of 4, so you could automate this change by creating a script or adding a line to a security template and importing the template into a domain-based Group Policy. The value is stored in: `HKLM\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ValidCommunities`.

### Potential Impact

You must also reconfigure the community string on all management tools that use the SNMP protocol.

**Disable NetBIOS and SMB on Public Facing Interfaces**

This section discusses specifically designed recommendations for servers that are located in networks that cannot be fully controlled, such as publicly accessible Web servers and e-mail gateways. These types of servers are often referred to as bastion hosts. If you have any such servers, you should consider the recommended procedures in this countermeasure. However, you should test each change thoroughly and ensure that you understand that it will be a challenge to manage computers on which NetBIOS has been disabled.

### Vulnerability

To help secure a bastion host, you can greatly reduce its attack surface if you disable server message block (SMB) and NetBIOS over TCP/IP. It will be difficult to manage servers that operate under this configuration, and they will be unable to access folders shared on the network. However, these measures effectively protect the server from compromise through the SMB and NetBIOS protocols. Therefore, you should disable SMB and NetBIOS over TCP/IP for network connections on servers that are accessible from the Internet.

### Countermeasure

SMB communication will not be prevented if you disable NetBIOS. SMB will use TCP port 445 (referred to as SMB Direct Host or the Common Internet File System (CIFS) port) in the absence of standard NetBIOS ports. As a result, explicit steps must be taken to disable both NetBIOS and SMB separately.

NetBIOS uses the following ports:
- **UDP/137** (NetBIOS name service)
- **UDP/138** (NetBIOS datagram service)
- **TCP/139** (NetBIOS session service)

SMB uses the following ports:
- **TCP/139**
- **TCP/445**

On servers that are accessible from the Internet, complete the following procedures to remove File and Printer Sharing for Microsoft Networks and Client for Microsoft Networks.
To disable SMB
1. In Control Panel, double-click **Network Connections**.
2. Right-click any Internet facing connection, and then click **Properties**.
3. In the **Properties** dialog box, click select **Client for Microsoft Networks**, and then click **Uninstall**.
4. Follow the uninstall steps.
5. Select **File and Printer Sharing for Microsoft Networks**, and then click **Uninstall**.
6. Follow the uninstall steps.

To disable NetBIOS over TCP/IP
1. In Control Panel, double-click **System**, click the **Hardware** tab, and then click the **Device Manager** button.
2. On the **View** menu, click **Show hidden devices**.
3. Expand **Non-Plug and Play Drivers**.
4. Right-click **NetBios over Tcpip**, and then click **Disable**.

These steps disable the SMB direct host listener on TCP/445 and UDP 445.

**Note**: This procedure disables the Nbt.sys driver. Although it disables the NetBIOS Session Service (which listens on TCP port 139), it does not disable SMB completely. To do so, follow the steps in the earlier "To disable SMB" procedure.

**Potential Impact**
No computers will be able to connect to the server through SMB. The servers will be unable to access folders shared on the network. Management tools that depend on NetBIOS or SMB for connectivity will be unable to connect to the servers.

**Configure Terminal Services Port**
Terminal Services is a useful tool for network administrators because it enables remote server and end-user computer management. The Remote Desktop client installs by default on all Windows Server 2003 and Windows XP computers, and it is available as an optional component on the Windows 2000 Server installation media. There is also a downloadable Microsoft ActiveX® client that runs within Internet Explorer or the Microsoft Management Console (MMC). The Remote Desktop and ActiveX clients are collectively known as the Terminal Services Advanced Client (TSAC).

**Vulnerability**
Terminal Services listens on TCP port 3389 by default, and all versions of the Remote Desktop clients attempt to connect to this port. Although the entire session (including the user authentication) is encrypted, Terminal Services clients do not perform server authentication. An attacker who was able to spoof a legitimate Terminal Services server could trick users and cause them to connect to the attacker's server instead of the genuine server. To achieve this deception, the attacker could alter DNS records to redirect users to their server or use some other means.

**Countermeasure**
Change the TCP port that is used by Terminal Services, or implement an IPsec policy to require trust and negotiate either Authentication Header (AH) or Encapsulation Security
Payload (ESP) using IPsec transport mode (not IPsec tunnel mode). In some scenarios, it may be feasible to isolate the Terminal Server behind a VPN gateway so that either Point-to-Point Tunneling Protocol (PPTP) or L2TP/IPSec-secured VPN tunnels are required to gain access to the Terminal Server.

For information about how to change the port that is used by Terminal Services and the Remote Desktop Client, see the Microsoft Knowledge Base article "How to Change Terminal Server's Listening Port" at http://support.microsoft.com/?scid=187623. This article explains how to change the listening port for the regular desktop client. To do so in the Terminal Services Advanced Client Web client, you need to add the following script line to the Web page:

```
MsRdpClient.RDPport = xxx
```

(xxx represents the desired TCP port number.) For more information about how you can use and customize Remote Desktop Web Connection to run Terminal Services sessions within Microsoft Internet Explorer, see "Providing for RDP Client Security" at http://msdn.microsoft.com/library/default.asp?url=/library/en-us/termserv/termserv/providing_for_rdp_client_security.asp.

**Potential Impact**

Implementation of IPsec with AH will have a negligible impact on computer performance, but it will introduce new overhead to manage client and server IPsec configuration. Additional overhead is also required to manage a mutual trust method between client and server computers that are used by Internet Key Exchange (IKE) security negotiation before IPsec security associations are established. The IPsec policy should be designed either to protect all traffic to the server, or to require IPsec just for connections to TCP port 3389. If you require IPsec on the server side, client computers that do not have a compatible IPsec configuration and trust will be denied access. See the "Configure IPsec Policies" section later in this chapter for more information about how to use IPsec policies to negotiate security for TCP/IP traffic.

If you change the default ports on Terminal Services servers and clients, legitimate users who do not have their client software configured to use the new port will not be able to connect to computers whose port assignments have been changed. Also, there is no way to change the TCP port in the current version of TSAC.

**Disable Dr. Watson: Disable Automatic Execution of Dr. Watson System Debugger**

System debuggers facilitate the troubleshooting of computers and applications. These programs gather data and present it to the system administrator or application developer while the computer is running. The Dr. Watson tool that is included with Windows Server 2003 and Windows XP is an automated system debugger that records information about the system state and applications that are active at the time that a program fault occurs.

**Vulnerability**

Some organizations may feel that no debuggers should be installed on critical production computers. There are no known Dr. Watson-related exploits that can be executed by users who do not have administrative privileges. In other words, an attacker would need to belong to the local **Administrators** group to use Dr. Watson as an attack tool against other users or processes. An attacker who has already gained administrative privileges has complete control of the computer, so attackers could still pursue other paths if you disable Dr. Watson.
Countermeasure

For instructions about how to disable the Dr. Watson system debugger, see the Microsoft Knowledge Base article "How to Disable Dr. Watson for Windows" at http://support.microsoft.com/?kbid=188296.

Potential Impact

No system debugger will run, and no report will be automatically created if programs crash. Systems administrators and developers will have less information available to them to diagnose the cause of such problems, and the error reporting feature will not work.

**Disable SSDP/UPNP: Disable SSDP/UPNP**

If you disable the Universal Plug and Play (UPnP™) host service, other applications such as Windows Messenger will still be able to use the Simple Service Discovery Protocol (SSDP) discovery service discovery process to identify network gateways or other network devices.

For more information, see the Microsoft Knowledge Base article "Traffic Is Sent After You Turn Off the SSDP Discover Service and Universal Plug and Play Device Host" at http://support.microsoft.com/?kbid=317843.

**Vulnerability**

The UPnP features included with Windows XP and Windows Server 2003 can be extremely useful for home users and small businesses because they can automate the installation and configuration of UPnP devices when they are attached to the local network. Some organizations may want to ensure that no UPnP or SSDP traffic travels across their network. Although there are no known vulnerabilities with these features right now, a major problem was discovered in Windows XP a couple of years ago that required application of a hotfix.

**Countermeasure**

To ensure that no applications use the SSDP and UPnP features that are included with Windows XP, you can add a REG_DWORD registry value called UPnPMode to the following registry key:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\DirectPlayNATHelp\DPNHUPnP\and configure its value to 2.
```

**Potential Impact**

UPnP and SSDP features will be completely disabled. When UPnP devices are attached to the network you will have to configure and manage them manually.

**Configure IPsec Policies**

IPsec (available in the Windows 2000, Windows XP, and the Microsoft Windows Server 2003 operating systems) is a tool that allows network security administrators to permit, block, or negotiate security for TCP/IP traffic. IPsec is independent of and transparent to applications. The design goal for Windows 2000 was
to provide a way to secure network traffic with the IPsec protocol's AH format or the ESP format. IPsec policy provides static TCP/IP traffic filters (also called selectors) that are necessary to negotiate security through IKE.


For most applications, the Windows Firewall component provides adequate host-level protection against malicious inbound traffic. The Security Configuration Wizard (SCW) in Windows Server 2003 with SP1 greatly simplifies the setup and management of Windows Firewall settings for large deployments. IPsec should be used to secure host-to-host and host-client traffic where appropriate, and Windows Firewall should typically be widely deployed within most organizations as an additional defensive layer.

Vulnerability

Although most network security strategies focus on how to prevent attacks from outside an organization's network, a great deal of sensitive information can be lost by internal attacks that interpret data on the network or that exploit design or implementation weaknesses in upper layer protocols to gain access to a computer. Attackers may use NetBT null sessions to gain information that could be used to compromise administrator passwords (if other security settings are not used or accidentally turned off).

Attackers simply need to locate one vulnerability in one application port to gain access and potentially full control of a computer. As noted, because many types of data are not protected when they travel across the network, employees, support staff members, or visitors may be able to copy data for later analysis. Firewalls that are located between the internal network and the Internet offer no protection against such internal threats. Internal firewalls often cannot provide authenticated access controls that are necessary to protect clients and servers, nor can they provide end-to-end security of network traffic between computers.

Countermeasure

IPsec filters recognize TCP/IP traffic by source and destination IP address, by IP protocol type, and by TCP and UDP ports. IPsec filters help contain and control the spread of malicious code because they block worm and virus traffic. Also, IPsec can make it very difficult for an attacker to use remote shells or other attack utilities to gain access to the computer from within a compromised application. For more details about how an IPsec policy can be applied in Windows 2000 to block ports, see the Microsoft Knowledge Base article "How to block specific network protocols and ports by using IPSec" at http://support.microsoft.com/?scid=813878. Also, the white paper "Using IPSec to Lock Down a Server" at www.microsoft.com/technet/itsolutions/network/security/ipsecld.mspx provides step-by-step configuration guidance for Windows Server 2003 IPsec permit/block filtering that is similar to this guidance. However, the NoDefaultExempt registry settings that are recommended by the Knowledge Base article should be added for Windows 2000.

Windows Server 2003 provides the MMC IPsec Policy Management snap-in, which is a graphical user interface (GUI) that you can use to manage IPsec policy. This tool is very similar to the one for Windows 2000 and Windows XP. Windows Server 2003 provides the MMC IPsec Monitor snap-in and the NETSH IPsec command-line utility to show the IPsec policy filters as they are applied on the computer. Permit and block filters appear in IKE Quick Mode configuration—IKE Quick Mode generic filters are the filters as defined in the assigned IPsec policy. IKE Quick Mode-specific filters result from the application of
policy to the particular IP configuration of the computer. Note that the IKE Quick Mode-specific function Find Matching Filters cannot be used to match permit and block filters, only filters that have a negotiate action.

The following terms are discussed in the rest of this section:

- **Filter List.** Includes ports, protocols, and directions. Filter lists trigger a decision when traffic matches something that is specified in the list. One list can contain multiple filters.

- **Filter Action.** The required response when traffic matches a filter list. Specific actions include blocking or permitting certain traffic.

- **Rule.** A rule is a correlation of a filter list with a filter action.

- **IPsec Policy.** A collection of rules. Only one policy can be active at any particular time.

An easy way to record this information is in a table called a network traffic map. A network traffic map contains basic information about the server role, the direction of network traffic, the destination of the traffic, the IP address of the interface, IP protocol, the TCP port, and the User Datagram Protocol (UDP) port that is involved. A sample network traffic map is shown in the following table.

A network traffic map helps you understand what types of network traffic enter and exit particular servers. Before you create IPsec policies, it is essential for you to understand what traffic is required for the server to function properly. Failure to do so may cause you to create filters that are too strict, which can cause application failures.

To create a traffic map

1. Determine the base network services that are required for the server role.

2. Identify the protocols and ports that are required by each service. This process may involve the use of Network Monitor to capture and analyze network traffic to determine destination addresses, protocols and ports. Also, you can use tools such as the Netstat.exe command to view open ports and active connections.

3. Document the IPsec filtering rules that are necessary to allow only the identified traffic.

If you start with the most restrictive IPsec filters and open up additional ports only as needed, the highest possible level of security can be achieved with these settings. This process is much easier if you divide the services into client and server services. The server services should be defined for any service that the computer provides to other hosts.

<table>
<thead>
<tr>
<th>Service</th>
<th>Protocol</th>
<th>Source port</th>
<th>Destination port</th>
<th>Source address</th>
<th>Destination address</th>
<th>Action</th>
<th>Mirror</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Server</td>
<td>TCP</td>
<td>ANY</td>
<td>80</td>
<td>ANY</td>
<td>ME</td>
<td>PERMIT</td>
<td>YES</td>
</tr>
<tr>
<td>HTTPS Server</td>
<td>TCP</td>
<td>ANY</td>
<td>443</td>
<td>ANY</td>
<td>ME</td>
<td>PERMIT</td>
<td>YES</td>
</tr>
<tr>
<td>DNS Client</td>
<td>TCP</td>
<td>ANY</td>
<td>53</td>
<td>ME</td>
<td>DNS</td>
<td>PERMIT</td>
<td>YES</td>
</tr>
<tr>
<td>Block everything</td>
<td>ANY</td>
<td>ANY</td>
<td>ANY</td>
<td>ANY</td>
<td>ANY</td>
<td>BLOCK</td>
<td>YES</td>
</tr>
</tbody>
</table>
In this sample traffic map, the Web server will provide HTTP and HTTPS services to computers from any source IP address, so appropriate traffic is permitted. The ME destination is interpreted by the IPsec service to create a filter for each of the IP addresses on the computer. Each of these filters will be mirrored to permit the traffic to return to the computer from which it originated. This approach effectively means that the HTTP Server rule will permit traffic that originates from any host on any source port to connect to port 80 on the IIS server. The mirror of this rule will permit TCP traffic from port 80 of the IIS server to go to any port on any host.

A client service can be any service that the computer performs in which the policies use another host. For example, in the sample traffic map, the server may need DNS client services to perform name lookups for one of the Web applications. In this example, a filter was created to permit traffic to and from the DNS server(s). Windows Server 2003 provides policy enhancements over Windows 2000 Server for this type of configuration to permit traffic to the DNS and other infrastructure servers. In Windows 2000, the IPsec policy must contain each of the DNS server IP addresses in the policy. In Windows Server 2003, the policy can use the logical name DNS, which will be expanded into a filter for each DNS server IP address based on the local IP configuration of the server.

**Note:** IPsec policies that use Windows Server 2003 features such as this one should not be assigned to Windows 2000 or Windows XP computers.

The mirrored block filter from Any IP to My IP Address will block all other unicast IP traffic to or from an IP address on the computer. This filter is more general than the protocol and port-specific filters that were defined for DNS, HTTP, and HTTPS. Because the default exemptions were removed for Windows Server 2003, this filter will match and therefore block outbound multicast and broadcast packets—because the source IP is My IP Address and the destination address matches Any IP address. However, note that inbound multicast and broadcast traffic is not matched by this filter. The source address would be Any IP, but the destination address of a multicast or broadcast packet is not a specific IP address on the computer—it is a multicast or broadcast IP address. Therefore, this rule will not block inbound multicast or broadcast traffic on Windows Server 2003. This filter definition is also supported by Windows 2000 and Windows XP. However, it will only match unicast IP traffic. Those platforms were not designed to match broadcast and multicast packets against IPsec filters. Therefore, outbound and inbound multicast and broadcast packets will be permitted even though this filter is applied on Windows 2000 and Windows XP computers.

The last rule, Block Everything, demonstrates another filter enhancement for Windows Server 2003. This rule is not supported by Windows 2000 or Windows XP. This rule blocks both inbound and outbound multicast and broadcast traffic as well as all other unicast traffic that does not match a more specific filter. If this rule is used, the previous “Any IP to Me” rule is not needed.

It is important to note that if such a policy were enforced, the computer could not communicate to its DHCP server to renew a lease, to domain controllers, to WINS servers, to CRL revocation sites, or to server monitoring stations. Also, this policy does not allow remote management by administrators who use RPC-based MMC snap-ins or a Remote Desktop client connection. Note also that if the example IIS server had two network interface cards—one for Internet access and one for internal access—all traffic over both interfaces would be filtered in the same manner. Therefore, this policy needs to be significantly customized to accommodate production environments. Network traffic should be filtered differently for the internal IP address or subnet. Filter rules that are used to require IPsec-encrypted remote management from specific management stations also should be used whenever possible so that other compromised servers cannot gain access to servers through the internal interface or capture administrative logon network traffic for offline attacks.
If a client service is required that cannot be restricted to connections with a particular destination server or a limited number of destination servers, the level of security provided by IPsec filters may be greatly reduced. In the following sample network traffic map, one rule is added so that an administrator can use a Web browser to access any Internet site for help information and to download patches. This capability requires a mirrored outbound static permit filter for TCP destination port 80 traffic.

Table 11.2 Sample Network Traffic Map that Allows Outbound Web Browsing

<table>
<thead>
<tr>
<th>Service</th>
<th>Protocol</th>
<th>Source port</th>
<th>Destination port</th>
<th>Source address</th>
<th>Destination address</th>
<th>Action</th>
<th>Mirror</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound ICMP for TCP PMTU</td>
<td>ICMP</td>
<td>ANY</td>
<td>ANY</td>
<td>ANY</td>
<td>ME</td>
<td>PERMIT</td>
<td>NO</td>
</tr>
<tr>
<td>Inbound IIS Server HTTP:80</td>
<td>TCP</td>
<td>ANY</td>
<td>80</td>
<td>ANY</td>
<td>ME</td>
<td>PERMIT</td>
<td>YES</td>
</tr>
<tr>
<td>Inbound IIS Server FTP:21</td>
<td>TCP</td>
<td>ANY</td>
<td>21</td>
<td>ANY</td>
<td>ME</td>
<td>PERMIT</td>
<td>YES</td>
</tr>
<tr>
<td>Inbound Terminal Server</td>
<td>TCP</td>
<td>ANY</td>
<td>3389</td>
<td>ANY</td>
<td>ME</td>
<td>PERMIT</td>
<td>YES</td>
</tr>
<tr>
<td>Me to Domain DCs all traffic</td>
<td>ANY</td>
<td>ANY</td>
<td>ANY</td>
<td>ME</td>
<td>Domain Name</td>
<td>PERMIT</td>
<td>YES</td>
</tr>
<tr>
<td>Outbound DNS UDP/TCP</td>
<td>UDP</td>
<td>ANY</td>
<td>53</td>
<td>ME</td>
<td>DNS</td>
<td>PERMIT</td>
<td>YES</td>
</tr>
<tr>
<td>Outbound DNS UDP/TCP</td>
<td>TCP</td>
<td>ANY</td>
<td>53</td>
<td>ME</td>
<td>DNS</td>
<td>PERMIT</td>
<td>YES</td>
</tr>
<tr>
<td>Outbound WINS</td>
<td>UDP</td>
<td>137</td>
<td>137</td>
<td>ME</td>
<td>WINS</td>
<td>PERMIT</td>
<td>YES</td>
</tr>
<tr>
<td>Outbound DHCP</td>
<td>UDP</td>
<td>68</td>
<td>67</td>
<td>ME</td>
<td>DHCP</td>
<td>PERMIT</td>
<td>YES</td>
</tr>
<tr>
<td>Outbound HTTP:80</td>
<td>TCP</td>
<td>ANY</td>
<td>80</td>
<td>ME</td>
<td>ANY</td>
<td>PERMIT</td>
<td>YES</td>
</tr>
<tr>
<td>Block everything</td>
<td>ANY</td>
<td>ANY</td>
<td>ANY</td>
<td>ANY</td>
<td>ANY</td>
<td>BLOCK</td>
<td>YES</td>
</tr>
</tbody>
</table>

Although this sample traffic map seems like a proper configuration, the result is that the entire policy now provides no security against an attacker who initiates an inbound connection from Any IP address through TCP source port 80. This attacker could access any open TCP port through the inbound permit filter, and the reply is allowed through the outbound permit filter back to TCP destination port 80.
Any of the following solutions could be used to block the inbound attack:

- Use additional IPsec filtering rules to block an attacker from using port 80 to gain inbound access to open ports.

- Use a front-end stateful filtering firewall or router to block inbound traffic from source port 80 unless it corresponds to an outbound connection.

- In addition to this IPsec policy, configure Windows Firewall on the server’s external network adapter to provide stateful filtering for all outbound traffic that is permitted by IPsec filters. Because Windows Firewall is layered above IPsec, Windows Firewall must also be configured to permit TCP ports 80 and 443 inbound (although this is the default configuration).

The sample traffic map in the following table uses additional IPsec filters to block any attempts to access open ports from port 80. First, the `netstat -ano` command is used to determine what TCP ports must be open on the server that the attacker could connect to. The output of this command is similar to the following:

C:\Documents and Settings\testuser.domain.000>netstat -ano

<table>
<thead>
<tr>
<th>Proto</th>
<th>Local Address</th>
<th>Foreign Address</th>
<th>State</th>
<th>PID</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>0.0.0.0:135</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>740</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:445</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>4</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:1025</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>884</td>
</tr>
<tr>
<td>TCP</td>
<td>0.0.0.0:1046</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>508</td>
</tr>
<tr>
<td>TCP</td>
<td>192.168.0.5:139</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>4</td>
</tr>
<tr>
<td>UDP</td>
<td>0.0.0.0:445</td>
<td><em>:</em></td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>UDP</td>
<td>0.0.0.0:500</td>
<td><em>:</em></td>
<td></td>
<td>508</td>
</tr>
<tr>
<td>UDP</td>
<td>0.0.0.0:1026</td>
<td><em>:</em></td>
<td></td>
<td>816</td>
</tr>
<tr>
<td>UDP</td>
<td>0.0.0.0:1029</td>
<td><em>:</em></td>
<td></td>
<td>508</td>
</tr>
<tr>
<td>UDP</td>
<td>0.0.0.0:1051</td>
<td><em>:</em></td>
<td></td>
<td>452</td>
</tr>
<tr>
<td>UDP</td>
<td>0.0.0.0:4500</td>
<td><em>:</em></td>
<td></td>
<td>508</td>
</tr>
<tr>
<td>UDP</td>
<td>127.0.0.1:123</td>
<td><em>:</em></td>
<td></td>
<td>884</td>
</tr>
<tr>
<td>UDP</td>
<td>192.168.0.5:123</td>
<td><em>:</em></td>
<td></td>
<td>884</td>
</tr>
<tr>
<td>UDP</td>
<td>192.168.0.5:137</td>
<td><em>:</em></td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>UDP</td>
<td>192.168.0.5:138</td>
<td><em>:</em></td>
<td></td>
<td>4</td>
</tr>
</tbody>
</table>

The rule is then defined to block the specific attack from TCP source port 25 to each open TCP port, as shown in the following table:
Table 11.3 Revised Sample Network Traffic Map that Allows Outbound Web Browsing

<table>
<thead>
<tr>
<th>Service</th>
<th>Protocol</th>
<th>Source port</th>
<th>Destination port</th>
<th>Source address</th>
<th>Destination address</th>
<th>Action</th>
<th>Mirror</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound ICMP for TCP PMTU</td>
<td>ICMP</td>
<td>ANY</td>
<td>ANY</td>
<td>ANY</td>
<td>ME</td>
<td>PERMIT</td>
<td>NO</td>
</tr>
<tr>
<td>Inbound IIS Server HTTP:80</td>
<td>TCP</td>
<td>ANY</td>
<td>80</td>
<td>ANY</td>
<td>ME</td>
<td>PERMIT</td>
<td>YES</td>
</tr>
<tr>
<td>Inbound IIS Server FTP:21</td>
<td>TCP</td>
<td>ANY</td>
<td>21</td>
<td>ANY</td>
<td>ME</td>
<td>PERMIT</td>
<td>YES</td>
</tr>
<tr>
<td>Inbound Terminal Server</td>
<td>TCP</td>
<td>ANY</td>
<td>3389</td>
<td>ANY</td>
<td>ME</td>
<td>PERMIT</td>
<td>YES</td>
</tr>
<tr>
<td>Me to Domain DCs all traffic</td>
<td>ANY</td>
<td>ANY</td>
<td>ANY</td>
<td>ME</td>
<td>Domain Name</td>
<td>PERMIT</td>
<td>YES</td>
</tr>
<tr>
<td>Outbound DNS UDP/TCP</td>
<td>UDP</td>
<td>ANY</td>
<td>53</td>
<td>ME</td>
<td>DNS</td>
<td>PERMIT</td>
<td>YES</td>
</tr>
<tr>
<td>Outbound DNS UDP/TCP</td>
<td>TCP</td>
<td>ANY</td>
<td>53</td>
<td>ME</td>
<td>DNS</td>
<td>PERMIT</td>
<td>YES</td>
</tr>
<tr>
<td>Outbound WINS</td>
<td>UDP</td>
<td>137</td>
<td>137</td>
<td>ME</td>
<td>WINS</td>
<td>PERMIT</td>
<td>YES</td>
</tr>
<tr>
<td>Outbound DHCP</td>
<td>UDP</td>
<td>68</td>
<td>67</td>
<td>ME</td>
<td>DHCP</td>
<td>PERMIT</td>
<td>YES</td>
</tr>
<tr>
<td>Outbound HTTP:80</td>
<td>TCP</td>
<td>ANY</td>
<td>80</td>
<td>ME</td>
<td>ANY</td>
<td>PERMIT</td>
<td>YES</td>
</tr>
<tr>
<td>Mitigation from inbound src 80</td>
<td>TCP</td>
<td>80</td>
<td>135</td>
<td>ANY</td>
<td>ME</td>
<td>BLOCK</td>
<td>NO</td>
</tr>
<tr>
<td>Mitigation from inbound src 80</td>
<td>TCP</td>
<td>80</td>
<td>139</td>
<td>ANY</td>
<td>ME</td>
<td>BLOCK</td>
<td>NO</td>
</tr>
<tr>
<td>Mitigation from inbound src 80</td>
<td>TCP</td>
<td>80</td>
<td>445</td>
<td>ANY</td>
<td>ME</td>
<td>BLOCK</td>
<td>NO</td>
</tr>
</tbody>
</table>
This example demonstrates how to create one-way filters to block traffic with a source port of 80 to any active ports on the computer, which would block an inbound attack. It prevents the ability to spoof a source port of 80 to connect to the ports that are required by RPC, NetBT, and SMB (CIFS).

You can apply IPsec policies in several ways:

- Apply them on an individual computer.
- Attach them to an OU or domain using Group Policy.
- Write a script for the `netsh ipsec` command, and then apply the script on select computers.

It is possible to distribute the IPsec policies based on Group Policy. However, when IPsec policies must be tailored to specific computers, it may be better to use local policies. Alternatively, a mix of local or domain based policy and NETSH IPsec-scripted persistent policy may be the most manageable. In particular, NETSH must be used to set persistent policy that provides security during computer startup. For more detailed information, see the section "Assigning Domain-based, OU-Level, and Local IPSec Policies" in Chapter 6, "Deploying IPSec" in the Windows Server 2003 Deployment Kit: Deploying Network Services.

**Negotiating IPSec Protection for Traffic**

The IKE protocol integration with IPsec filtering permits policy-based, automatic negotiation of IPsec cryptograhic protection for unicast IP traffic that matches the IPsec filters. IPsec-protected packets can either use the AH format or the ESP format with security options determined by policy configuration. The use of IPsec policies to negotiate IPsec-secured transport for upper layer protocols and applications provides the following benefits:

- Defense in depth against network attacks. IPsec is a mature, state-of-the-art, security protocol that was designed by the Internet Engineering Task Force (IETF). It allows you to add a strong layer of defense at a layer beneath all unicas t IP communications to augment application-based security. In this way, IPsec defends against vulnerabilities in the security of upper-layer protocols and can significantly strengthen communications security. For example, the SMB file-sharing protocol is used extensively for Active Directory® directory service replication, file transfer, printing, and Group Policy download. However, SMB does not provide privacy. All data that is sent inside SMB is visible to the passive network observer. SMB does provide digital signing, although in some cases it is not feasible to require because one setting
Threats and Countermeasures

affects all SMB communication paths. IPsec can be applied to secure a specific network path or set of paths. Two identified SMB security issues were identified in Windows 2000 and Windows XP. Although supported fixes for these security issues are now available from Microsoft, you can enhance security if you use IPsec as a first layer of defense against attacks on SMB or other protocols. For more information about the two identified SMB security vulnerabilities and supported fixes for Windows 2000 and Windows XP, see the following Microsoft Knowledge Base articles:

- “MS02-070: Flaw in SMB Signing May Permit Group Policy to Be Modified” at http://support.microsoft.com/?kbid=329170.

• Host–based authentication and encryption for all traffic between two or more computers to ensure that the administrative owner of the data retains full control of the data as it traverses the network. The data in network traffic contains core information assets that are vital and proprietary to the owners. The theft of this information as it flows through the network could cause catastrophic damage to the business or mission of the organization. If business and legal trust relationships that manage the trust and integrity of the network path are not enforced perfectly, or are silently compromised, the IPsec-encrypted communications remain secured.

• Simple and secure firewall traversal. The many protocols that are used in communications between domain controllers, between servers, or between clients and servers are interpreted by firewalls only as IPsec ESP (protocol 50) traffic or as AH (protocol 51) traffic. The firewalls can be configured to permit only traffic for these protocols (and IKE traffic), and these protocols are hardened against attacks.

• IPsec that uses the 3DES encryption algorithm and the SHA1 integrity algorithm is certified under the Common Criteria and FIPS 140-1. Many government, military, financial, and health care institutions require that Common Criteria or FIPS 140-1-certified algorithms be used to secure their traffic. The RC4 stream cipher algorithm is used by default to encrypt traffic over most Windows protocols, such as RPC, the Kerberos authentication protocol, and Lightweight Directory Access Protocol (LDAP). RC4 is not one of the Common Criteria or FIPS 140-1-certified algorithms.

• As a software–based Windows solution, IPsec is a more cost-effective way to secure host-to-host communications than a hardware-based solution. Hardware-based security solutions, such as a virtual private network (VPN) or a private leased line, may be more expensive than the use of Windows IPsec.

• IPsec can provide lower CPU utilization than protocol-specific security measures such as SMB signing. Network adapters that offload IPsec processing accelerate the cryptographic operations that are used to secure IPsec packets, which minimizes the performance costs for encryption. As a result, IPsec-secured TCP/IP connections can achieve the same throughput as TCP/IP connections that are not secured with IPsec—although these adapters may add equipment costs. If such adapters cannot be used, then IPsec encryption will increase the CPU load on a domain controller. This increased CPU load may or may not require additional CPU capacity, which will depend on the available CPU and the amount of network traffic. You will need to conduct performance tests assess the impact on the domain controllers in specific scenarios. For more information about the benefits of IPsec hardware offload adapters, see “Intel PRO/100S Network Adapter, IPSec Offload Performance and Comparison” at www.veritest.com/clients/reports/intel/intelps.pdf.

Potential Impact

IPsec is one tool that you can use to harden a server against network attack. It should not be viewed as the only tool or a complete solution. IPsec filtering was not designed to
replace the need for a full-featured perimeter firewall or router filters. It is recommended only for simple packet filtering scenarios to harden clients and servers where static filters can be effective. Also, IPsec filtering was designed for a directory-based policy to apply to many computers. Therefore, the MMC IPsec Policy Management snap-in cannot provide detailed information during the configuration process about how a policy will be applied to a specific computer. Limitations of IPsec filtering include the following:

- IPsec filters cannot be applied for a particular application. They can only be defined for protocols and ports that the application uses.
- IPsec filters are static. They do not provide “stateful” outbound traffic filtering. To permit outbound network traffic typically requires a static outbound and inbound permit filter. Therefore, IPsec cannot defend against an attacker who uses the static inbound permit filter to gain access to any open port. Therefore, outbound permit filters should be specific only to the IP address or range that is required.
- IPsec filters do not differentiate between different types of ICMP messages.
- IPsec filters do not perform inspection of the contents of IP packets for the purpose of intrusion detection.
- IPsec filters can overlap, but cannot be manually ordered. The IPsec service internally calculates a weight that provides an automatic filter order. The address part of the filter takes precedence first, then the protocol, then the source and destination ports.
- IPsec filters are not interface-specific. They can be configured to be IP address-specific, but all traffic on each interface will be matched against the filter list.
- IPsec filters cannot be explicitly configured as inbound or outbound. The inbound and outbound direction is automatically determined based on the addresses that are specified in the filter. In some cases, both inbound and outbound filters are generated automatically.
- IPsec policy does not support duplicate filters.
- Although Windows Server 2003 substantially improved the performance of IPsec filtering, host-based filtering may add CPU load for very large traffic volumes. An optimized front-end router or firewall may provide faster filtering of traffic.

When IPsec (or other network device) filtering blocks network traffic, unusual application behavior and event messages may result. IPsec filtering does not provide an easy-to-read log of dropped inbound and outbound traffic. Network Monitor (Netmon) captures of network traffic cannot view outbound traffic that is blocked. Although Netmon can view inbound traffic that is blocked, there is no indication in the capture file that a particular packet is dropped. Effective diagnostics depend upon the knowledge of normal application behavior, events, and network traffic flows when IPsec policy is not assigned.

Furthermore, the proper design of IPsec filters for application traffic may depend upon detailed analysis of network traffic flows to understand how the application uses the network. For example, the SMB protocol uses TCP port 139 for file transfer, file sharing, and print sharing. If this port is blocked by IPsec, SMB can also use TCP port 445. Another example is when an application requires multiple network traffic flows to different destinations. SMB and other protocols typically authenticate the user, which can transparently cause the computer to locate and exchange Kerberos traffic with the domain controller. The Kerberos protocol uses DNS UDP 53 or TCP 53 to discover a list of domain controller IP addresses, then LDAP UDP 389 and UDP and TCP port 88 to potentially any of the domain controller IP addresses. Therefore, a print failure may actually be caused by a blocked packet to the domain controller. Some protocols, such as RPC, use a wide range of TCP ports that are dynamically determined when a computer starts, or at the time an application is executed, which means that RPC
applications cannot be effectively controlled by static filters on ports except when the RPC application provides the configuration to require the use of a static port.

In Windows 2000 and Windows XP, default exemptions to filters that are specified in the policy configuration were designed for IP network traffic types that either cannot be secured with IKE (broadcast and multicast IP packets), must be exempt for quality of service (QoS) to be provided for IPsec traffic (RSVP protocol), and must be required by the IPsec system to function (IKE itself and the Kerberos protocol as an IKE authentication method). Although a registry key was provided to remove them, these exemptions were often not disabled when IPsec filters were used for permit and block firewall scenarios. Therefore, Windows Server 2003 only provides an exemption for IKE traffic. Microsoft recommends that you remove the default exemptions for all IPsec scenarios that use Windows 2000 and Windows XP. For more information about default exemptions, see the Microsoft Knowledge Base article "IPSec Default Exemptions Can Be Used to Bypass IPSec Protection in Some Scenarios" at http://support.microsoft.com/?kbid=811832 and Microsoft Knowledge Base article "IPSec default exemptions are removed in Windows Server 2003" at http://support.microsoft.com/?kbid=810207.

When a Windows 2000 computer is connected to the Internet, a mirrored outbound permit filter (such as for port 80, which was explained earlier in this chapter) allows an attacker to gain access to any open TCP port on the server from the Internet through the source port. Therefore, a mistake in IPsec configuration may result in loss of expected security. Configurations should be tested to ensure that they provide the expected security and protection from attacks.

A security compromise that allows an attacker to obtain either Local Administrator or Local System access could allow them to disable or change the IPsec policy.

IPsec in Windows 2000 does not provide complete filtering during computer startup. There is a small window of time in which the TCP/IP stack is responsive. An automated attack could potentially access application ports that the IPsec policy would otherwise block. In most cases, applications have not been able to start processing connections before IPsec filtering was in place. To achieve the highest level of security when using IPsec filtering, you should disconnect the computer from the network during restart.

Windows Server 2003 provides an initial startup policy that the IPsec driver uses when loaded by TCP/IP during computer startup. When the IPsec service starts, it immediately applies persistent policy. Then, when a local or domain policy assignment can be determined, the service applies this policy assignment in addition to the persistent policy. Therefore, a NETSH IPsec script that configures a secure default persistent policy (for example, block all traffic except management traffic) can provide complete protection during transition from startup to local or domain-assigned IPsec policy. More information is available in the Windows Server 2003 online Help and in the deployment kit.

However, neither Windows 2000 nor Windows Server 2003 is designed to allow you to configure service dependencies on the IPsec Policy Agent service startup. Configuration of a service dependency does not effectively guarantee that the filters are in place before the dependent service starts.

Windows Server 2003 and Windows XP with SP2 provide the Windows Firewall service, which performs stateful filtering for outbound traffic and provides basic controls for inbound access to ports and ICMP message types. Windows Firewall also provides a readable log of inbound and outbound blocked packets. Administrators should investigate Windows Firewall capabilities to determine if it better suits their needs for filtering traffic. The stateful filtering that is provided by Windows Firewall can be used in combination with IPsec filtering to protect scenarios in which IPSec must be configured to use mirrored outbound filters to permit traffic. Front-end router or firewall filtering should be used as the first line of defense when feasible.
A host-based intrusion detection system and other antivirus systems are worth consideration to detect and potentially defend against infection and attacks within permitted network traffic and applications. A third party host–based or edge firewall may provide the best solution for complex filtering needs.

**Negotiating IPsec Protection for Traffic**

Although IPsec end-to-end protection can greatly enhance security, if you deploy IPsec-secured communications on your network you will incur additional training and administrative costs. It may also involve additional hardware costs if you need to purchase IPsec hardware, offload network adapters, or increase CPU capacity. Therefore, before you deploy IPsec for any specific scenario, you should carefully consider and document the potential security threats that IPsec is intended to address, your security requirements, the costs of IPsec deployment, and the expected business benefits.

Implementation of IPsec with AH introduces new overhead to manage a client/server IPsec configuration as well as to manage a mutual trust method between client/server computers. If the two computers are always in the same domain or mutually trusted domains, then Group Policy can deliver the necessary IPsec policy settings and Kerberos authentication can establish trust for IPsec security associations. If computers are not able to use Kerberos authentication, then either computer certificates or a preshared authentication key may be used. However, this guide does not recommend preshared authentication keys because the key value is stored unprotected in the IPsec policy configuration.

Although the local IPsec policy can only be read by administrators who defined the policy, policy that is stored in Active Directory needs to be accessible by all domain computers. Therefore, it is difficult to maintain privacy of the preshared key value. Microsoft recommends the use of digital certificates when the Kerberos protocol cannot be used for IKE authentication. IPsec policy should be designed to either protect all traffic, or to negotiate IPsec just for specific TCP or UDP ports. IPsec policy on the client side typically must be configured with the server’s static IP address. If you require IPsec on the server side, access would be denied to client computers that did not have a compatible IPsec policy configuration and mutual trust method.

Configuring Windows Firewall

An Internet firewall can help prevent outsiders from accessing your computer through the Internet. Windows XP with SP2 and Windows Server 2003 with SP1 include the Windows Firewall, a built-in firewall that can provide for many organizations an additional layer of protection against network-based attacks such as worms and denial-of-service attacks.

1. Click Start, and then click Control Panel.
2. Click Windows Firewall.
3. Click the On (recommended) radio button.
4. If necessary, click the Exceptions tab and configure exceptions for protocols that you want to allow through the firewall.
5. Click OK to activate Windows Firewall.

Windows Firewall does not have the rich feature set that is provided by many third-party products, because it is intended only as a basic intrusion prevention feature. Windows Firewall does not allow people to gather data about the PC and blocks unsolicited connection attempts. However, Windows Firewall does not do extensive outbound filtering.

Windows Firewall adds several key improvements over the Internet Connection Firewall (ICF) that was included in earlier versions of Windows. In particular, Windows Firewall can be centrally managed through Group Policy. For information about available management tools and settings, see the "Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2" white paper at www.microsoft.com/downloads/details.aspx?FamilyID=4454e0e1-61fa-447a-bdcd-499f73a637d1&DisplayLang=en.
More Information

The following links provide additional information about additional hardening measures for Windows Server 2003 and Windows XP:


- The *Microsoft Internet Security and Acceleration (ISA) Server 2004 Hardening Guide* that is available for download at http://download.microsoft.com/download/c/e/c/cecc8742-2102-42d4-9fc7-6b641bebbf56/ISASecurityGuide.doc describes the necessary steps to harden an ISA Server 2004 computer, regardless of whether it is a domain member.

- The "Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2" white paper at www.microsoft.com/downloads/details.aspx?FamilyID=4454e0e1-61fa-447a-bdcd-499f73a637d1 outlines a process to help you determine the appropriate settings for Windows Firewall and how to deploy them.
Conclusion

This guide explained the most significant security countermeasures that are available in Microsoft® Windows Server™ 2003 with SP1 and Microsoft Windows® XP Professional with SP2. You can create a security template and import it into a Group Policy object (GPO) that is linked to the parent organizational unit (OU) for the member server to manage most of the recommended settings. Many other settings can be implemented through configuration of the Administrative Templates (ADM) sections of Group Policy. However, because some hardening procedures cannot be applied through Group Policy, the guide also discussed some manual configuration settings.

More Information

• For more information about security and privacy at Microsoft, see the Security page at www.microsoft.com/security.


• For more information about common network attack types, see "Common Types of Network Attacks," extracted from the Windows 2000 Server Resource Kit, which is available online at www.microsoft.com/resources/documentation/Windows/2000/server/reskit/en-us/cnet/cnbd_ips_ddui.asp.

• For more information about how to harden the Windows Server 2003 TCP/IP stack, see the Microsoft Knowledge Base article "How to Harden the TCP/IP Stack Against Denial of Service Attacks in Windows Server 2003" at http://support.microsoft.com/?scid=324270.
For more information about how to harden the settings for Windows Sockets applications, see the Microsoft Knowledge Base article "Internet Server Unavailable Because of Malicious SYN Attacks" at http://support.microsoft.com/?scid=142641.

For more information about the location of .adm files, see the Microsoft Knowledge Base article "Location of ADM (Administrative Template) Files in Windows" at http://support.microsoft.com/?scid=228460.


For more information about the architecture that underlies the creation, editing, and processing of security templates, see “How Security Settings Extension Works” at www.microsoft.com/technet/prodtechnol/windowsserver2003/library/TechRef/f546e58e-8473-4985-a05d-0b038dea4a9f.mspx. This article includes detailed information about Group Policy storage, precedence, and how some settings persist even when a particular Group Policy is no longer applied to a computer (often referred to colloquially as ‘tattooing’).

For more information about how to customize the Security Configuration Editor user interface, see the Microsoft Knowledge Base article “How to Add Custom Registry Settings to Security Configuration Editor” at http://support.microsoft.com/?scid=214752.

For more information about how to create custom administrative template files in Windows, see the Microsoft Knowledge Base article “How to: Create Custom Administrative Templates in Windows 2000” at http://support.microsoft.com/?scid=323639.

For more information about how to ensure that more secure LAN Manager Authentication Level settings work in networks with a mix of Windows 2000 and Windows NT® 4.0 computers, see the Microsoft Knowledge Base article “Authentication Problems in Windows 2000 with NTLM 2 Levels Above 2 in a Windows NT 4.0 Domain” at http://support.microsoft.com/?scid=305379.

For more information about LAN Manager compatibility levels, see the Microsoft Knowledge Base article "Client, service, and program incompatibilities that may occur when you modify security settings and user rights assignments” at http://support.microsoft.com/?scid=823659.

For more information about NTLMv2 authentication, see the Microsoft Knowledge Base article "How to Enable NTLM 2 Authentication" at http://support.microsoft.com/?scid=239869.


• For more information about user rights assignments for Windows Server 2003, see the User Rights Assignment page at www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/uratopnode.mspx.

• For more information about how to secure Terminal Services, see “Securing Windows 2000 Terminal Services.” The information in this article is also relevant to Windows Server 2003, and is available at www.microsoft.com/technet/prodtechnol/win2kts/maintain/optimize/secw2kts.asp.

• For more information about how to restore default security settings locally, see Microsoft Knowledge Base article “How to Reset Security Settings Back to the Defaults” at http://support.microsoft.com/?scid=313222.

• For more information about how to restore default security settings in the built-in domain Group Policy objects, see Microsoft Knowledge Base Article “How to Reset User Rights in the Default Domain Group Policy in Windows Server 2003” at http://support.microsoft.com/?scid=324800.

• For more information about security in the various Windows operating systems, see the Microsoft Windows Security Resource Kit. Information about purchasing this book is available from Microsoft Press at www.microsoft.com/MSPress/books/6418.asp.

Acknowledgments

The Microsoft Solutions for Security and Compliance group (MSSC) would like to acknowledge and thank the team that produced Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP. The following people were either directly responsible or made a substantial contribution to the writing, development, and testing of this solution.

Authors
Mike Danseglio
Kurt Dillard
José Maldonado
Paul Robichaux (3Sharp, LLC)

Content Contributors
Liam Colvin (3Sharp, LLC)
William Dixon (V6 Security Inc.)
Tony Dowler (3Sharp, LLC)
Eric Fitzgerald
Devin Ganger (3Sharp, LLC)
Jesper Johansson
Brad Warrender

Program Manager
Bomani Siwatu

Release Manager
Flicka Crandell

Editors
Reid Bannecker
John Cobb (Volt Information Sciences)
Jon Tobey (Volt Information Sciences)
Steve Wacker (Wadeware LLC)

Reviewers
Roger Abell (Arizona State University)
Rich Benack
Susan Bradley (SBS MVP)
Buz Brodin
Steve Clark
Curtis Clay III
Karel Dekyvere
Christine Duell (Valente Solutions)
Robert Hensing
Don McGowan
James Noyce
(Principal Consultant, Business Critical Consulting)

Testers
Kenon Bliss (Volt Information Sciences)
Paresh Gujar (Infosys Technologies)
Vince Humphreys (Volt Information Sciences)
Ashish Java (Infosys Technologies)
Mehul Mediwal (Infosys Technologies)
Rob Pike
Debra Littlejohn Shinder (Security MVP)
Tom Shinder
(ISA and Security MVP and IT Consultant TACTeam)
Ben Smith
Jeff Williams
Jim Whitney (Configuresoft)
Other Contributors

Ignacio Avellaneda
Ganesh Balakrishnan
Tony Bailey
Nathan Buggia
Derick Campbell
Chase Carpenter
Jeff Cohen
John Dwyer
Karl Grunwald
Joanne Kennedy
Karina Larson (Volt Information Sciences)
Chrissy Lewis (Siemens Business Services)
Kelly McMahon (Content Master Ltd.)

David Mowers
Jeff Newfeld
Rob Oikawa
Peter Meister
Bill Reid
Sandeep Sinha
Stacy Tsurusaki (Volt Information Sciences)
David Visintainer (Volt Information Sciences)
Rob Wickham
Graham Whiteley
Lori Woehler
Jay Zhang

At the request of Microsoft, The Center for Internet Security (CIS) and the United States Department of Commerce National Institute of Standards and Technology (NIST) participated in the final review of these Microsoft documents and provided comments, which were incorporated into the published versions.