the CENTER for
INTERNET SECURITY

Windows XP Professional

Operating System Legacy, Enterprise, and Specialized Security Benchmark Consensus Baseline Security Settings

Version 2.01
August, 2005

http://www.cisecurity.org

Editors: Jeff Shawgo
Sidney Faber
Nancy Whitney
windows-feedback@lists.cisecurity.org

Table of Contents

Terms of Use Agreement

Background.

The Center for Internet Security ("**CIS**") provides benchmarks, scoring tools, software, data, information, suggestions, ideas, and other services and materials from the CIS website or elsewhere (“**Products**”) as a public service to Internet users worldwide. Recommendations contained in the Products (“**Recommendations**”) result from a consensus-building process that involves many security experts and are generally generic in nature. The Recommendations are intended to provide helpful information to organizations attempting to evaluate or improve the security of their networks, systems, and devices. Proper use of the Recommendations requires careful analysis and adaptation to specific user requirements. The Recommendations are not in any way intended to be a “quick fix” for anyone’s information security needs.

No Representations, Warranties, or Covenants.

CIS makes no representations, warranties, or covenants whatsoever as to (i) the positive or negative effect of the Products or the Recommendations on the operation or the security of any particular network, computer system, network device, software, hardware, or any component of any of the foregoing or (ii) the accuracy, reliability, timeliness, or completeness of the Products or the Recommendations. CIS is providing the Products and the Recommendations “as is” and “as available” without representations, warranties, or covenants of any kind.

User Agreements.

By using the Products and/or the Recommendations, I and/or my organization (“**We**”) agree and acknowledge that:

1. No network, system, device, hardware, software, or component can be made fully secure;
2. We are using the Products and the Recommendations solely at our own risk;
3. We are not compensating CIS to assume any liabilities associated with our use of the Products or the Recommendations, even risks that result from CIS’s negligence or failure to perform;
4. We have the sole responsibility to evaluate the risks and benefits of the Products and Recommendations to us and to adapt the Products and the Recommendations to our particular circumstances and requirements;
5. Neither CIS, nor any CIS Party (defined below) has any responsibility to make any corrections, updates, upgrades, or bug fixes; or to notify us of the need for any such corrections, updates, upgrades, or bug fixes; and
6. Neither CIS nor any CIS Party has or will have any liability to us whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages (including without limitation loss of profits, loss of sales, loss of or damage to reputation, loss of customers, loss of software, data, information or emails, loss of privacy, loss of

use of any computer or other equipment, business interruption, wasted management or other staff resources or claims of any kind against us from third parties) arising out of or in any way connected with our use of or our inability to use any of the Products or Recommendations (even if CIS has been advised of the possibility of such damages), including without limitation any liability associated with infringement of intellectual property, defects, bugs, errors, omissions, viruses, worms, backdoors, Trojan horses or other harmful items.

Grant of Limited Rights.

CIS hereby grants each user the following rights, but only so long as the user complies with all of the terms of these Agreed Terms of Use:

1. Except to the extent that we may have received additional authorization pursuant to a written agreement with CIS, each user may download, install and use each of the Products on a single computer;
2. Each user may print one or more copies of any Product or any component of a Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, provided that all such copies are printed in full and are kept intact, including without limitation the text of this Agreed Terms of Use in its entirety.

Retention of Intellectual Property Rights; Limitations on Distribution.

The Products are protected by copyright and other intellectual property laws and by international treaties. We acknowledge and agree that we are not acquiring title to any intellectual property rights in the Products and that full title and all ownership rights to the Products will remain the exclusive property of CIS or CIS Parties. CIS reserves all rights not expressly granted to users in the preceding section entitled “Grant of limited rights.”

Subject to the paragraph entitled “Special Rules” (which includes a waiver, granted to some classes of CIS Members, of certain limitations in this paragraph), and except as we may have otherwise agreed in a written agreement with CIS, we agree that we will not (i) decompile, disassemble, reverse engineer, or otherwise attempt to derive the source code for any software Product that is not already in the form of source code; (ii) distribute, redistribute, encumber, sell, rent, lease, lend, sublicense, or otherwise transfer or exploit rights to any Product or any component of a Product; (iii) post any Product or any component of a Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device, without regard to whether such mechanism or device is internal or external, (iv) remove or alter trademark, logo, copyright or other proprietary notices, legends, symbols or labels in any Product or any component of a Product; (v) remove these Agreed Terms of Use from, or alter these Agreed Terms of Use as they appear in, any Product or any component of a Product; (vi) use any Product or any component of a Product with any derivative works based directly on a Product or any component of a Product; (vii) use any Product or any component of a Product with other products or applications that are directly and specifically dependent on such Product or any component for any part of their functionality, or (viii) represent or claim a particular level of compliance with a CIS Benchmark, scoring tool or other Product. We will not facilitate or otherwise aid other individuals or entities in any of the activities listed in this paragraph.

We hereby agree to indemnify, defend, and hold CIS and all of its officers, directors, members, contributors, employees, authors, developers, agents, affiliates, licensors, information and service providers, software suppliers, hardware suppliers, and all other persons who aided CIS in the creation, development, or maintenance of the Products or Recommendations ("**CIS Parties**") harmless from and against any and all liability, losses, costs, and expenses (including attorneys' fees and court costs) incurred by CIS or any CIS Party in connection with any claim arising out of any violation by us of the preceding paragraph, including without limitation CIS's right, at our expense, to assume the exclusive defense and control of any matter subject to this indemnification, and in such case, we agree to cooperate with CIS in its defense of such claim. We further agree that all CIS Parties are third-party beneficiaries of our undertakings in these Agreed Terms of Use.

Special Rules.

The distribution of the NSA Security Recommendations is subject to the terms of the NSA Legal Notice and the terms contained in the NSA Security Recommendations themselves (http://www.nsa.gov/ia).

CIS has created and will from time to time create, special rules for its members and for other persons and organizations with which CIS has a written contractual relationship. Those special rules will override and supersede these Agreed Terms of Use with respect to the users who are covered by the special rules.

CIS hereby grants each CIS Security Consulting or Software Vendor Member and each CIS Organizational User Member, but only so long as such Member remains in good standing with CIS and complies with all of the terms of these Agreed Terms of Use, the right to distribute the Products and Recommendations within such Member's own organization, whether by manual or electronic means. Each such Member acknowledges and agrees that the foregoing grant is subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Choice of Law; Jurisdiction; Venue

We acknowledge and agree that these Agreed Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland, that any action at law or in equity arising out of or relating to these Agreed Terms of Use shall be filed only in the courts located in the State of Maryland, that we hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action. If any of these Agreed Terms of Use shall be determined to be unlawful, void, or for any reason unenforceable, then such terms shall be deemed severable and shall not affect the validity and enforceability of any remaining provisions.

WE ACKNOWLEDGE THAT WE HAVE READ THESE AGREED TERMS OF USE IN THEIR ENTIRETY, UNDERSTAND THEM, AND WE AGREE TO BE BOUND BY THEM IN ALL RESPECTS.

Quick Start Instructions

Just a few years ago, it was almost impossible to find a reliable source for Windows security. Since then, the momentum has shifted in the opposite direction – there is a wealth of information available. Now the questions are, "Which published source do I trust as authoritative? What should MY standard be?"

One side-effect of this wealth of information available is that there are local computer security experts who want to toss the documentation aside, and apply the standards. I have one piece of advice before you go and do that:

IF YOU ONLY READ ONE PAGE IN THIS GUIDE, READ THIS PAGE!

This guide imposes changes that are best implemented in a managed environment. They are designed to limit communication between computers to positively identified and authorized personnel. This is a change from the normal way of thinking in a Windows world. Major systems should still function, but testing this benchmark in a controlled environment is essential.

I want to run the tool now!

It is understandable to want to "hit the ground running". If you want to run the accompanying tool this very minute, go ahead and do so. Please look through the accompanying "Readme.txt" file. The tool is designed to measure the status of your system against a standard, and score it accordingly. The tool will not make changes to the security settings on your system, except that it must be installed as an application.

For The Seasoned Security Professional

More and more Windows support personnel are becoming familiar with the intricacies of Windows security. Microsoft itself has stated an organizational shift of its priorities away from ease-of-use toward security awareness.

Section 1 of this guide is a summary checklist of the configuration settings that constitute a Windows XP Professional compliant computer system. It is brief and to the point. Appendix A is a questionnaire that can be used to put the trade-offs into perspective for each of the settings involved.

For the Windows User Seeking Enlightenment

Computer and network security is a difficult topic to summarize. Many of the features that are enabled "out of the box" on a Windows computer are enabled "in case" the prospective owner wants to use them. Most of these features never get used, but often still have vulnerabilities that can be exploited by unscrupulous people.

Section 2 of this guide is written to provide contextual descriptions of each requirement for this benchmark. It gives plain-text details of what the setting means, why it is restricted, and what the consequences of restricting that setting may be. It covers the same information as Section 1, in greater detail. You should still use the questionnaire in Appendix A to explore some of the trade-offs of implementing these settings.

Windows XP Professional Benchmark
Consensus Baseline Security Settings

August 2005

This document is a security benchmark for the Microsoft Windows XP Professional operating system for workstations. It reflects the content of the Consensus Baseline Security Settings document developed by the National Security Agency (NSA), the Defense Information Systems Agency (DISA), The National Institute of Standards and Technology (NIST), the General Services Administration (GSA), The SANS Institute, and the staff and members of the Center for Internet Security (CIS).

Intended Audience

This benchmark is intended for anyone using a Windows XP Professional operating system who feels at all responsible for the security of that system. A Security Manager or Information Security Officer should certainly be able to use this guide and the associated tools to gather information about the security status of a network of Windows machines. The owner of a small business or home office can use this guide as a straightforward aid in enhancing his or her own personal network security. A Windows System Administrator can use this guide and the associated tools to produce explicit scores that can be given to management to reflect where they currently stand, versus where they should stand with regard to security.

Any user who uses this guide to make even the slightest improvement on the secure state of a system might be doing just enough to turn a potential hacker or cracker away to an easier target. Every computer operator who becomes “Security Aware” improves the safety level of the Internet.

Practical Application

Just as there is often no single correct way to get to a specific destination, there is more than one way to implement the settings and suggestions described in this text. In a network environment, with a Windows 2000 or Windows 2003 Active Directory Domain, Group Policy can be used to apply nearly all the settings described herein. Many surveys of Fortune 500 or Fortune 1000 companies have indicated that large companies have been slow to migrate to Active Directory because of the level of complexity involved, but the lack of continued support for Windows NT 4.0 Domains is fueling the migration process. Once an infrastructure has been implemented to support an Active Directory domain, implementing most of these policies with Group Policy becomes relatively easy.

In an environment where Active Directory isn’t in use, administrators and users are forced to use the Local Security Policy editor of individual Member Servers and Workstations to lock down their environment.

The information contained in this text applies equally well to Local Security Policies and to Group Policies. In a large domain infrastructure, Group Policy can (and should) be set to override the Local Security Policy. Anyone attempting to make modifications to the Local Security Policy which seem to “mysteriously disappear” should contact their system administrator or their management to see if Group Policy may be overriding their changes.

The actions required to “harden” a Windows operating system will be described in terms of updating the Local Security Policy. The Local Security Policy Editor, as well as many other tools used herein, is located in the Administrative Tools menu. In some cases, clicking the Start button, and then looking under Programs will be enough. Otherwise, click Start, Settings, and open the Control Panel. Double-click the Administrative Tools icon in the Control Panel to find the Local Security Policy Editor.

Keeping Score

The goal of every benchmark and the associated scoring tools is to give users a point-in-time view of where systems stand in relation to the currently accepted standard. This “score” produced by the scoring tool is a number between 0 and 100.

The criteria used for scoring are divided into five categories: (1) Service Packs and Security Updates, (2) Auditing and Account Policies, (3) Security Settings, (4) Additional Security Protection, and (5) Administrative Templates. Additional applications or Services may detract from the overall score, just as additional services detract from the security of these systems in the production environment.

Security Levels

One question that needs to be considered when securing computers is "How secure should they be?" Often people assume that the highest level of security is best, but it is important to remember that often, a vulnerability is defended by disabling some functionality. The use of this function may be more important to the usefulness of the computer than defending against the vulnerability.

In response to this, CIS is publishing three different levels of guidance.

Legacy - Settings in this level are designed for XP Professional systems that need to operate with older systems such as Windows NT, or in environments where older third party applications are required. The settings will not affect the function or performance of the operating system or of applications that are running on the system.

Enterprise Desktop - Settings in this level are designed for XP Professional systems operating in a managed environment where interoperability with legacy systems is not required. It assumes that all operating systems within the enterprise are Windows 2000 or later, therefore able to use all possible security features available within those systems. In such environments, these Enterprise-level settings are not likely to affect the function or performance of the OS. However, one should carefully consider the possible impact to software applications when applying these recommended XP Professional technical controls.

Enterprise Mobile - These settings are nearly identical to the Enterprise Standalone settings, but with modifications appropriate for mobile users whose systems must operate both on and away from the corporate network. In environments where all systems are Windows 2000 or later, these Enterprise-level settings are not likely to affect the function or performance of the OS. However, one should carefully consider the possible impact to software applications when applying these recommended XP Professional technical controls.

Specialized Security – Limited Functionality – Formerly known as "High Security," settings in this level are designed for XP Professional systems in which security and integrity are the highest priorities, even at the expense of functionality, performance, and interoperability. Therefore, each setting should be considered carefully and only applied by an experienced administrator who has a thorough understanding of the potential impact of each setting or action in a particular environment.

Section 1 – Summary Checklist

Setting:	Legacy	Enterprise		Specialized Security – Limited Functionality
		Desktop	Mobile	
1 Service Packs and Security Updates				
1.1 Major Service Pack and Security Update Requirements				
1.1.1 Current Service Pack Installed	Service Pack 2 as of this writing			
1.2 Minor Service Pack and Security Update Requirements				
1.2.1 Security Updates as referred by Microsoft Security Bulletins	All Critical and Important Security Updates			
2 Auditing and Account Policies				
2.1 Major Auditing and Account Policies Requirements				
2.1.1 Minimum Password Length	8 Characters			12 Characters
2.1.2 Maximum Password Age	90 Days			
2.2 Minor Auditing and Account Policies Requirements				
2.2.1 Audit Policy (minimums)				
2.2.1.1 Audit Account Logon Events	Success and Failure			
2.2.1.2 Audit Account Management	Success and Failure			
2.2.1.3 Audit Directory Service Access	<Not Defined>			
2.2.1.4 Audit Logon Events	Success and Failure			
2.2.1.5 Audit Object Access	Failure (minimum)			Success and Failure
2.2.1.6 Audit Policy Change	Success (minimum)			
2.2.1.7 Audit Privilege Use	Failure (minimum)			
2.2.1.8 Audit Process Tracking	<Not Defined>			

Setting:	Legacy	Enterprise		Specialized Security – Limited Functionality
		Desktop	Mobile	
2.2.1.9 Audit System Events	Success (minimum)			
2.2.2 Account Policy				
2.2.2.1 Minimum Password Age	1 day			
2.2.2.2 Maximum Password Age	90 days			
2.2.2.3 Minimum Password Length	8 characters			12 characters
2.2.2.4 Password Complexity	Enabled			
2.2.2.5 Password History	24 passwords remembered			
2.2.2.6 Store Passwords using Reversible Encryption	Disabled			
2.2.3 Account Lockout Policy				
2.2.3.1 Account Lockout Duration	15 minutes			15 minutes
2.2.3.2 Account Lockout Threshold	50 attempts			10 attempts
2.2.3.3 Reset Account Lockout After	15 minutes			15 minutes
2.2.4 Event Log Settings – Application, Security, and System Logs				
2.2.4.1 Application Log				
2.2.4.1.1 Maximum Event Log Size	16 MB			
2.2.4.1.2 Restrict Guest Access	Enabled			
2.2.4.1.3 Log Retention Method	As Needed			
2.2.4.1.4 Log Retention	<Not Defined>			
2.2.4.2 Security Log				
2.2.4.2.1 Maximum Event Log Size	80 MB			
2.2.4.2.2 Restrict Guest	Enabled			

Setting:	Legacy	Enterprise		Specialized Security – Limited Functionality
		Desktop	Mobile	
Access				
2.2.4.2.3 Log Retention Method	As Needed			
2.2.4.2.4 Log Retention	<Not Defined>			
2.2.4.3 System Log				
2.2.4.3.1 Maximum Event Log Size	16 MB			
2.2.4.3.2 Restrict Guest Access	Enabled			
2.2.4.3.3 Log Retention Method	As Needed			
2.2.4.3.4 Log Retention	<Not Defined>			
3 Security Settings				
3.1 Major Security Settings				
3.1.1 Network Access: Allow Anonymous SID/Name Translation:	Disabled			
3.1.2 Network Access: Do not allow Anonymous Enumeration of SAM Accounts	Enabled			
3.1.3 Network Access: Do not allow Anonymous Enumeration of SAM Accounts and Shares	Enabled			
3.1.4 Data Execution Protection	Enabled			
3.2 Minor Security Settings				
3.2.1 Security Options				
3.2.1.1 Accounts: Administrator Account Status	<Not Defined>	<Not Defined>		<Not Defined>

Setting:	Legacy	Enterprise		Specialized Security – Limited Functionality
		Desktop	Mobile	
3.2.1.2 Accounts: Guest Account Status	Disabled			
3.2.1.3 Accounts: Limit local account use of blank passwords to console logon only	Enabled			
3.2.1.4 Accounts: Rename Administrator Account	<User Defined Value>			
3.2.1.5 Accounts: Rename Guest Account	<User Defined Value>			
3.2.1.6 Audit: Audit the access of global system objects	<Not Defined>			Disabled
3.2.1.7 Audit: Audit the use of backup and restore privilege	<Not Defined>			Disabled
3.2.1.8 Audit: Shut Down system immediately if unable to log security alerts	<Not Defined>			
3.2.1.9 DCOM: Machine Access Restrictions (SP2 only)	<Not Defined>			
3.2.1.10 DCOM: Machine Launch Restrictions (SP2 only)	<Not Defined>			
3.2.1.11 Devices: Allow undock without having to log on	<Not Defined>			Disabled
3.2.1.12 Devices: Allowed to format and eject removable media	Administrators, Interactive Users			Administrators
3.2.1.13 Devices: Prevent users from installing printer drivers	<Not Defined>	Enabled	<Not Defined>	Enabled
3.2.1.14 Devices: Restrict CD-ROM Access to Locally Logged-On User Only	<Not Defined>			Disabled
3.2.1.15 Devices: Restrict Floppy Access to Locally Logged-On	<Not Defined>			Disabled

Setting:	Legacy	Enterprise		Specialized Security – Limited Functionality
		Desktop	Mobile	
User Only				
3.2.1.16 Devices: Unsigned Driver Installation Behavior	Warn, but allow…			
3.2.1.17 Domain Controller: Allow Server Operators to Schedule Tasks	<Not Applicable>			
3.2.1.18 Domain Controller: LDAP Server Signing Requirements	<Not Applicable>			
3.2.1.19 Domain Controller: Refuse machine account password changes	<Not Applicable>			
3.2.1.20 Domain Member: Digitally Encrypt or Sign Secure Channel Data (Always)	Disabled	Enabled		
3.2.1.21 Domain Member: Digitally Encrypt Secure Channel Data (When Possible)	Enabled			
3.2.1.22 Domain Member: Digitally Sign Secure Channel Data (When Possible)	Enabled			
3.2.1.23 Domain Member: Disable Machine Account Password Changes	Disabled			
3.2.1.24 Domain Member: Maximum Machine Account Password Age	30 days			
3.2.1.25 Domain Member: Require Strong (Windows 2000 or later) Session Key	<Not Defined>	Enabled		
3.2.1.26 Interactive Logon: Do Not Display Last User Name	Enabled			
3.2.1.27 Interactive Logon: Do not require CTRL+ALT+DEL	Disabled			

Setting:	Legacy	Enterprise		Specialized Security – Limited Functionality
		Desktop	Mobile	
3.2.1.28 Interactive Logon: Message Text for Users Attempting to Log On	<Custom, or DoJ Approved>			
3.2.1.29 Interactive Logon: Message Title for Users Attempting to Log On	<Custom, or DoJ Approved>			
3.2.1.30 Interactive Logon: Number of Previous Logons to Cache	2	2	2	0
3.2.1.31 Interactive Logon: Prompt User to Change Password Before Expiration	14 days			
3.2.1.32 Interactive Logon: Require Domain Controller authentication to unlock workstation	<Not Defined>	Enabled	Disabled	<Not Defined>
3.2.1.33 Interactive Logon: Smart Card Removal Behavior	Lock Workstation			
3.2.1.34 Microsoft Network Client: Digitally sign communications (always)	<Not Defined>	Enabled		
3.2.1.35 Microsoft Network Client: Digitally sign communications (if server agrees)	Enabled			
3.2.1.36 Microsoft Network Client: Send Unencrypted Password to Connect to Third-Party SMB Server	Disabled			
3.2.1.37 Microsoft Network Server: Amount of Idle Time Required Before Disconnecting Session	15 Minutes			
3.2.1.38 Microsoft Network Server: Digitally sign communications (always)	<Not Defined>	Enabled		
3.2.1.39 Microsoft Network Server:	Enabled			

Setting:	Legacy	Enterprise		Specialized Security – Limited Functionality
		Desktop	Mobile	
Digitally sign communications (if client agrees)				
3.2.1.40 Microsoft Network Server: Disconnect clients when logon hours expire	Enabled		Disabled	Enabled
3.2.1.41 Network Access: Do not allow storage of credentials or .NET passports for network authentication	<Not Defined>	Enabled		
3.2.1.42 Network Access: Let Everyone permissions apply to anonymous users	Disabled			
3.2.1.43 Network Access: Named pipes that can be accessed anonymously	<Not Defined>	COMNAP COMNODE SQL\QUERY SPOOLSS LLSRPC browser		
3.2.1.44 Network Access: Remotely accessible registry paths	<Not Defined>			System\CurrentControlSet\Control\ProductOptions, System\CurrentControlSet\Control\Print\Printers, System\CurrentControlSet\Control\Server Applications, System\CurrentControlSet\Services\Eventlog, Software\Microsoft\OLAP Server, Software\Microsoft\Windows NT\CurrentVersion, System\CurrentControlSet\Control\ContentIndex, System\CurrentControlSet\Control\Terminal Server, System\CurrentControlSet\Co

Setting:	Legacy	Enterprise		Specialized Security – Limited Functionality
		Desktop	Mobile	
				ntrol\Terminal Server\UserConfig, System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration
3.2.1.45 Network Access: Shares that can be accessed anonymously	<Not Defined>			COMCFG, DFS$
3.2.1.46 Network Access: Sharing and security model for local accounts	Classic			
3.2.1.47 Network Security: Do not store LAN Manager password hash value on next password change	<Not Defined>	Enabled		
3.2.1.48 Network Security: Force logoff when logon hours expire	<Not Defined>	Enabled	<Not Defined>	Enabled
3.2.1.49 Network Security: LAN Manager Authentication Level	Send NTLMv2	Send NTLMv2, refuse LM		Send NTLMv2, refuse LM and NTLM
3.2.1.50 Network Security: LDAP client signing requirements	Negotiate Signing			
3.2.1.51 Network Security: Minimum session security for NTLM SSP based (including secure RPC) clients	<Not Defined>	Require Message Integrity, Message Confidentiality, NTLMv2 Session Security, 128-bit Encryption		
3.2.1.52 Network Security: Minimum session security for NTLM SSP based (including secure RPC) servers	<Not Defined>	Require Message Integrity, Message Confidentiality, NTLMv2 Session Security, 128-bit Encryption		
3.2.1.53 Recovery Console: Allow Automatic Administrative Logon	Disabled			
3.2.1.54 Recovery Console: Allow Floppy Copy and Access to All	<Not Defined>			Disabled

Setting:	**Legacy**	**Enterprise**		**Specialized Security – Limited Functionality**
		Desktop	**Mobile**	
Drives and All Folders				
3.2.1.55 Shutdown: Allow System to be Shut Down Without Having to Log On	Disabled			
3.2.1.56 Shutdown: Clear Virtual Memory Pagefile	<Not Defined>			Enabled
3.2.1.57 System Cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	<Not Defined>			
3.2.1.58 System objects: Default owner for objects created by members of the Administrators group	CREATOR OWNER			
3.2.1.59 System objects: Require case insensitivity for non-Windows subsystems	<Not Defined>			Enabled
3.2.1.60 System objects: Strengthen default permissions of internal system objects	<Not Defined>	Enabled		
3.2.2 Additional Registry Settings				
3.2.2.1 Suppress Dr. Watson Crash Dumps: **HKLM\Software\Microsoft\DrWatson\CreateCrashDump**	<Not Defined>			(REG_DWORD) 0
3.2.2.2 Disable Automatic Execution of the System Debugger: **HKLM\Software\Microsoft\Windows NT\CurrentVersion\AEDebug\Auto**	<Not Defined>			
3.2.2.3 Disable autoplay from any disk type, regardless of application: **HKLM\Software\Microsoft\Windows\CurrentVersion\**	(REG_DWORD) 255			

Setting:	Legacy	Enterprise		Specialized Security – Limited Functionality
		Desktop	Mobile	
Policies\Explorer\ NoDriveTypeAutoRun				
3.2.2.4 Disable autoplay for current user: **HKCU\Software\ Microsoft\Windows\ CurrentVersion\Policies\ Explorer\ NoDriveTypeAutoRun**	(REG_DWORD) 255			
3.2.2.5 Disable autoplay for the default profile: **HKU\.DEFAULT\ Software\Microsoft\Windows\ CurrentVersion\Policies\ Explorer\NoDriveTypeAutoRun**	(REG_DWORD) 255			
3.2.2.6 Disable Automatic Logon: **HKLM\Software\Microsoft\ Windows NT\CurrentVersion\ Winlogon\AutoAdminLogon**	<Not Defined>			
3.2.2.7 Disable automatic reboots after a Blue Screen of Death: **HKLM\System\CurrentControl Set\Control\CrashControl\ AutoReboot**	<Not Defined>			(REG_DWORD) 0
3.2.2.8 Disable CD Autorun: **HKLM\System\CurrentControl Set\ Services\CDrom\Autorun (REG_DWORD)**	(REG_DWORD) 0			
3.2.2.9 Remove administrative shares on workstation (Professional): **HKLM\System\ CurrentControlSet\Services\ LanmanServer\Parameters\ AutoShareWks**	<Not Defined>			0
3.2.2.10 Protect against Computer	<Not Defined>			

Setting:	Legacy	Enterprise		Specialized Security – Limited Functionality
		Desktop	Mobile	
Browser Spoofing Attacks: **HKLM\System\ CurrentControlSet\Services\ MrxSmb\Parameters\ RefuseReset**				
3.2.2.11 Protect against source-routing spoofing: **HKLM\System\ CurrentControlSet\Services\ Tcpip\Parameters\ DisableIPSourceRouting**	(REG_DWORD) 2			
3.2.2.12 Protect the Default Gateway network setting: **HKLM\System\ CurrentControlSet\Services\Tcpip\Parameters\ EnableDeadGWDetect**	<Not Defined>			(REG_DWORD) 0
3.2.2.13 Ensure ICMP Routing via shortest path first: **HKLM\System\ CurrentControlSet\Services\ Tcpip\Parameters\ EnableICMPRedirect**	<Not Defined>			(REG_DWORD) 0
3.2.2.14 Help protect against packet fragmentation: **HKLM\System\ CurrentControlSet\Services\ Tcpip\Parameters\ EnablePMTUDiscovery**	<Not Defined>			
3.2.2.15 Manage Keep-alive times: **HKLM\System\ CurrentControlSet\Services\ Tcpip\Parameters\ KeepAliveTime**	<Not Defined>			(REG_DWORD) 300000
3.2.2.16 Protect Against Malicious	<Not Defined>	<Not Defined>		(REG_DWORD) 1

Setting:	Legacy	Enterprise		Specialized Security – Limited Functionality
		Desktop	Mobile	
Name-Release Attacks: **HKLM\System\ CurrentControlSet\Services\ Netbt\Parameters\ NoNameReleaseOnDemand**				
3.2.2.17 Ensure Router Discovery is Disabled: **HKLM\System\CurrentControlSet\Services\Tcpip\ Parameters\PerformRouterDiscovery (REG_DWORD)**	<Not Defined>			(REG_DWORD) 0
3.2.2.18 Protect against SYN Flood attacks: **HKLM\System\ CurrentControlSet\Services\ Tcpip\Parameters\ SynAttackProtect**	<Not Defined>			(REG_DWORD) 2
3.2.2.19 SYN Attack protection – Manage TCP Maximum half-open sockets: **HKLM\System\ CurrentControlSet\Services\ Tcpip\Parameters\ TcpMaxHalfOpen**	<Not Defined>			
3.2.2.20 SYN Attack protection – Manage TCP Maximum half-open retired sockets: **HKLM\System\CurrentControlSet\Services\ Tcpip\Parameters\TcpMaxHalfOpenRetired (REG_DWORD)**	<Not Defined>			
3.2.2.21 Enable IPSec to protect Kerberos RSVP Traffic: **HKLM\System\**	(REG_DWORD) 1			

Setting:	Legacy	Enterprise		Specialized Security – Limited Functionality
		Desktop	Mobile	
CurrentControlSet\Services\ IPSEC\ NoDefaultExempt				
3.2.2.22 Hide workstation from Network Browser listing: **HKLM\System\ CurrentControlSet\Services\ Lanmanserver\Parameters\ Hidden**	<Not Defined>			(REG_DWORD) 1
3.2.2.23 Enable Safe DLL Search Mode: **HKLM\System\ CurrentControlSet\Control\ Session Manager\ SafeDllSearchMode**	(REG_DWORD) 1			
3.2.2.24 Disable WebDAV basic authentication (SP 2 only): **HKLM\System\CurrentControlSet\Services\WebClient\Parameters\UseBasicAuth**	(REGDWORD) 1			
3.2.2.25 Disable basic authentication over a clear channel (SP 2 only): **HKLM\SOFTWARE\Microsoft\ Windows\CurrentVersion\Internet Settings\DisableBasicOverClearChannel**	<Not Defined>			(REGDWORD) 1
3.2.2.26 USB Block Storage Device Policy (SP2 only): **HKLM\System\CurrentControlSet\Control\StorageDevicePolicies**	<Not Defined>			(REGDWORD) 1
3.2.2.27 DTC Access (SP2 only): **HKLM\Software\Microsoft\MSDTC**	<Not Defined>			(REGDWORD) 0

Setting:	Legacy	Enterprise		Specialized Security – Limited Functionality
		Desktop	Mobile	
4 Additional Security Protection				
4.1 Available Services (Permissions on services listed here: Administrators: Full Control; System: Read, Start, Stop, and Pause)				
4.1.1 Alerter	Disabled			
4.1.2 Automatic Updates	<Not Defined>			
4.1.3 Background Intelligent Transfer Service	<Not Defined>			
4.1.4 Clipbook	Disabled			
4.1.5 Computer Browser	<Not Defined>		Disabled	
4.1.6 Fax Service	<Not Defined>			Disabled
4.1.7 FTP Publishing Service	Disabled			
4.1.8 IIS Admin Service	Disabled			
4.1.9 Indexing Service	<Not Defined>			Disabled
4.1.10 Messenger	Disabled			
4.1.11 Net Logon	<Not Defined>			
4.1.12 NetMeeting Remote Desktop Sharing	Disabled			
4.1.13 Remote Desktop Help Session Manager	<Not Defined>	<Not Defined>		Disabled
4.1.14 Remote Registry Service	<Not Defined>			
4.1.15 Routing and Remote Access	Disabled			
4.1.16 Simple Mail Transfer Protocol (SMTP)	Disabled			
4.1.17 Simple Network Management Protocol (SNMP) Service	Disabled			

Setting:	Legacy	Enterprise		Specialized Security – Limited Functionality
		Desktop	Mobile	
4.1.18 Simple Network Management Protocol (SNMP) Trap	Disabled			
4.1.19 Task Scheduler	<Not Defined>			Disabled
4.1.20 Telnet	Disabled			
4.1.21 Terminal Services	<Not Defined>			Disabled
4.1.22 Universal Plug and Play Device Host	<Not Defined>	Disabled		
4.1.23 World Wide Web Publishing Services	Disabled			
4.2 User Rights				
4.2.1 Access this computer from the network	<Not Defined>	<Not Defined>		
4.2.2 Act as part of the operating system	<None>			
4.2.3 Add workstations to domain	<Not Applicable>			
4.2.4 Adjust memory quotas for a process	<Not Defined>			
4.2.5 Allow logon through terminal services	<Not Defined>			<None>
4.2.6 Back up files and directories	<Not Defined>			
4.2.7 Bypass traverse checking	<Not Defined>			
4.2.8 Change the system time	Administrators			
4.2.9 Create a pagefile	Administrators			
4.2.10 Create a token object	<None>			
4.2.11 Create permanent shared objects	<None>			
4.2.12 Debug Programs	Administrators	Administrators		<None>
4.2.13 Deny access to this computer from the network	Guests, Support_388945a0			
4.2.14 Deny logon as a batch job	<Not Defined>			

Setting:	Legacy	Enterprise		Specialized Security – Limited Functionality
		Desktop	Mobile	
4.2.15 Deny logon as a service	<Not Defined>			
4.2.16 Deny logon locally	<Not Defined>			
4.2.17 Deny logon through Terminal Service	<Not Defined>			
4.2.18 Enable computer and user accounts to be trusted for delegation	<Not Applicable>			
4.2.19 Force shutdown from a remote system	Administrators			
4.2.20 Generate security audits	Local Service, Network Service			
4.2.21 Increase scheduling priority	Administrators			
4.2.22 Load and unload device drivers	Administrators			
4.2.23 Lock pages in memory	<None>			
4.2.24 Log on as a batch job	<Not Defined>			
4.2.25 Log on as a service	<Not Defined>			
4.2.26 Log on locally	Users, Administrators			
4.2.27 Manage auditing and security log	Administrators			
4.2.28 Modify firmware environment values	Administrators			
4.2.29 Perform volume maintenance tasks	Administrators			
4.2.30 Profile single process	Administrators			
4.2.31 Profile system performance	Administrators			
4.2.32 Remove computer from docking station	Users, Administrators			
4.2.33 Replace a process level token	Local Service, Network Service			
4.2.34 Restore files and directories	Administrators			

Setting:	Legacy	Enterprise		Specialized Security – Limited Functionality
		Desktop	Mobile	
4.2.35 Shut down the system	Users, Administrators			
4.2.36 Synchronize directory service data	<Not Applicable>			
4.2.37 Take ownership of file or other objects	Administrators			
4.3 Other System Requirements				
4.3.1 Ensure volumes are using the NTFS file system	All volumes			
4.3.2 Disable NetBIOS	<Not Defined>	<Not Defined>		
4.3.3 Enable the Internet Connection Firewall	<Not Defined> but Strongly Recommended			
4.3.4 Restricted Groups	Remote Desktop Users: <None>			
4.4 File				
4.4.1 File Permissions				
4.4.1.1 %SystemRoot%\system32\at.exe	Administrators: Full; System: Full			
4.4.1.2 %SystemRoot%\system32\attrib.exe	Administrators: Full; System: Full			
4.4.1.3 %SystemRoot%\system32\cacls.exe	Administrators: Full; System: Full			
4.4.1.4 %SystemRoot%\system32\debug.exe	Administrators: Full; System: Full			
4.4.1.5 %SystemRoot%\system32\drwatson.exe	Administrators: Full; System: Full			
4.4.1.6 %SystemRoot%\system32\drwtsn32.exe	Administrators: Full; System: Full			
4.4.1.7 %SystemRoot%\system32\edlin.exe	Administrators: Full; System: Full; Interactive: Full			

Setting:	Legacy	Enterprise		Specialized Security – Limited Functionality
		Desktop	Mobile	
4.4.1.8 %SystemRoot%\system32\ eventcreate.exe	Administrators: Full; System: Full			
4.4.1.9 %SystemRoot%\system32\ eventtriggers.exe	Administrators: Full; System: Full			
4.4.1.10 %SystemRoot%\system32\ ftp.exe	Administrators: Full; System: Full; Interactive: Full			Administrators: Full; System: Full
4.4.1.11 %SystemRoot%\system32\ net.exe	Administrators: Full; System: Full; Interactive: Full			Administrators: Full; System: Full
4.4.1.12 %SystemRoot%\system32\ net1.exe	Administrators: Full; System: Full; Interactive: Full			Administrators: Full; System: Full
4.4.1.13 %SystemRoot%\system32\ netsh.exe	Administrators: Full; System: Full			
4.4.1.14 %SystemRoot%\system32\ rcp.exe	Administrators: Full; System: Full			
4.4.1.15 %SystemRoot%\system32\ reg.exe	Administrators: Full; System: Full			
4.4.1.16 %SystemRoot%\regedit.exe	Administrators: Full; System: Full			
4.4.1.17 %SystemRoot%\system32\ regedt32.exe	Administrators: Full; System: Full			
4.4.1.18 %SystemRoot%\system32\ regsvr32.exe	Administrators: Full; System: Full			
4.4.1.19 %SystemRoot%\system32\ rexec.exe	Administrators: Full; System: Full			
4.4.1.20 %SystemRoot%\system32\ rsh.exe	Administrators: Full; System: Full			
4.4.1.21 %SystemRoot%\system32\ runas.exe	Administrators: Full; System: Full; Interactive: Full			Administrators: Full; System: Full
4.4.1.22 %SystemRoot%\system32\ sc.exe	Administrators: Full; System: Full			

Setting:	Legacy	Enterprise		Specialized Security – Limited Functionality
		Desktop	Mobile	
4.4.1.23 %SystemRoot%\system32\subst.exe	Administrators: Full; System: Full			
4.4.1.24 %SystemRoot%\system32\telnet.exe	Administrators: Full; System: Full; Interactive: Full			Administrators: Full; System: Full
4.4.1.25 %SystemRoot%\system32\tftp.exe	Administrators: Full; System: Full; Interactive: Full			Administrators: Full; System: Full
4.4.1.26 %SystemRoot%\system32\tlntsvr.exe	Administrators: Full; System: Full			
5 Administrative Templates				
5.1 System				
5.1.1 Remote Procedure Call				
5.1.1.1 RPC Endpoint Mapper Client Authentication (SP2 only)	<Not Defined>			Enabled
5.1.1.2 Restrictions for Unauthenticated RPC clients (SP2 only)	<Not Defined>			Enabled; Authenticated without exceptions
5.2 Network				
5.2.1 Network Connections				
5.2.1.1 Windows Firewall				
5.2.1.1.1 Domain Profile				
5.2.1.1.1.1 Protect all network connections (SP2 only)	Enabled			Enabled
5.2.1.1.1.2 Do not allow exceptions (SP2 only)	Disabled			Enabled
5.2.1.1.1.3 Allow local program exceptions	Enabled			Disabled
5.2.1.1.1.4 Allow remote administration	Enabled; define subnet(s) used for internal support only			Disabled

Setting:	Legacy	Enterprise		Specialized Security – Limited Functionality
		Desktop	Mobile	
exception				
5.2.1.1.1.5 Allow file and printer sharing exception (SP2 only)	Enabled			Disabled
5.2.1.1.1.6 Allow ICMP exceptions (SP2 only)	<Not Defined>			Disabled
5.2.1.1.1.7 Allow Remote Desktop exception (SP2 only)	Enabled; define subnet(s) used for internal support only			Disabled
5.2.1.1.1.8 Allow UPnP framework exception (SP2 only)	Enabled; define subnet(s) used for internal support only			Disabled
5.2.1.1.1.9 Prohibit notifications	Disabled			Enabled
5.2.1.1.1.10 Log dropped packets (SP2 only)	Log dropped packets			Log dropped packets
5.2.1.1.1.11 Log file path and name (SP2 only)	Log file path and name: %SystemRoot%\firewall_domain.log			Log file path and name: %SystemRoot%\firewall_domain.log
5.2.1.1.1.12 Log file size limit (SP2 only)	Size Limit (KB): 4096			Size Limit (KB): 4096
5.2.1.1.1.13 Log successful connections (SP2 only)	<Not Defined>			Log successful connections
5.2.1.1.1.14 Prohibit unicast response to multicast or broadcast (SP2 only)	Enabled			Enabled
5.2.1.1.1.15 Define port exceptions (SP2 only)	<Not Configured>			<Not Configured>

Setting:	Legacy	Enterprise		Specialized Security – Limited Functionality
		Desktop	Mobile	
5.2.1.1.1.16 Allow local port exceptions (SP2 only)	Enabled			Disabled
5.2.1.1.2 Standard Profile				
5.2.1.1.2.1 Protect all network connections (SP2 only)	Enabled			Enabled
5.2.1.1.2.2 Do not allow exceptions (SP2 only)	Enabled			Enabled
5.2.1.1.2.3 Allow local program exceptions(SP2 only)	Disabled			Disabled
5.2.1.1.2.4 Allow remote administration exception (SP2 only)	Disabled			Disabled
5.2.1.1.2.5 Allow file and printer sharing exception (SP2 only)	Disabled			Disabled
5.2.1.1.2.6 Allow ICMP exceptions (SP2 only)	Enabled; Allow outbound source quench Allow inbound echo request Allow outbound packet too big			Disabled
5.2.1.1.2.7 Allow Remote Desktop exception (SP2 only)	Disabled			Disabled
5.2.1.1.2.8 Allow UPnP framework exception (SP2 only)	Disabled			Disabled
5.2.1.1.2.9 Prohibit notifications (SP2 only)	Disabled			Enabled
5.2.1.1.2.10 Log Dropped Packets (SP2 only)	Log dropped packets			Log dropped packets

Setting:	**Legacy**	**Enterprise**		**Specialized Security – Limited Functionality**
		Desktop	**Mobile**	
5.2.1.1.2.11 Log file path and name (SP2 only)	Log file path and name: %SystemRoot%\firewall_standard.log			Log file path and name: %SystemRoot%\firewal_standard.log
5.2.1.1.2.12 Log file size limit (SP2 Only)	Size Limit (KB): 4096			Size Limit (KB): 4096
5.2.1.1.2.13 Log Successful Connections (SP2 only)	<Not Defined>			Log successful connections
5.2.1.1.2.14 Prohibit unicast response to multicast or broadcast (SP2 only)	Enabled			Enabled
5.2.1.1.2.15 Define port exceptions (SP2 only)	<Not Configured>			<Not Configured>
5.2.1.1.2.16 Allow local port exceptions (SP2 only)	Disabled			Disabled
5.3 Windows Components				
5.3.1 Security Center				
5.3.1.1 Turn on Security Center (Domain PCs Only) (SP2 only)	Enabled			Enabled

Section 2 – Expanded Descriptions of Security Modifications

1 Service Packs and Security Updates

Microsoft periodically distributes large updates to its operating systems in the form of Service Packs, as often as once every few months, or less frequently. Service Packs include all major and minor fixes up to the date of the service pack, and are extensively tested by Microsoft prior to release. In light of the vast number of applications available, it is entirely possible that a bug in a Service Pack may not be discovered, and may slip through this engineering analysis process. Service Packs should be used in a test environment before being pushed into production. If a test system is not available, wait a week or two after the release of a Service Pack, and pay attention to the Microsoft web site for potential bug reports. Additional mailing list and Internet resources are listed in the appendices of this document.

It is important to be aware that Service Packs and Security Updates are not just applicable to operating systems. Individual applications have their own Service Pack and Security Update requirements. A Windows system that is completely current on Windows Security Updates and Service Packs also needs to be kept current with Service Packs and Security Updates for Internet Explorer and Microsoft Office. The total security of the system requires attention to both Operating System and application levels.

In addition to Service Packs, Microsoft issues many other software updates. For example, non-security bugs are corrected with a hotfix, and new features are released with a feature pack. Microsoft issues security updates when a vulnerability is identified in one of their products. If a number of hotfixes, security updates and other code updates are available for a product, Microsoft may choose to bundle all these software updates together in an update rollup.

Security updates can be released within hours of discovery of any particular bug or vulnerability, because they address a single problem. Since they may be released quickly, they do not pass the rigorous regression testing involved with Service Packs. They should be used with caution at first, even more so than Service Packs. Each security update includes a description of the issue it resolves.

1.1 Major Service Pack and Security Update Requirements

1.1.1 Current Service Pack installed

At the time of this writing, Windows XP Service Pack 2 is available.

WARNING: Although Service Packs are generally reliable and go through extensive testing, it is possible that it is not compatible with every software product on the market. If possible, test service packs in a test environment, or at least wait until it has been released for a short while before installing it, and watch for industry feedback on the compatibility of that service pack.

1.2 Minor Service Pack and Security Update Requirements

1.2.1 All Critical and Important Security Updates available to date have been installed.

WARNING: Although security updates are generally reliable and go through some testing, it is significantly possible that a security update addressing a single problem is not compatible with every software product on the market, and may cause other problems. If possible, test security updates in a test environment, or at least wait until they have been released for a short while before installation, and watch for industry feedback on the compatibility of those security updates.

2 Auditing and Account Policies

2.1 Major Auditing and Account Policies Requirements

2.1.1 Password Length

In general, password length and password complexity requirements are used to protect against password guessing attacks. These attacks are relatively unsophisticated: the crack is simply to make repeated guesses to see if the correct password has been chosen. The attack is usually performed in a manner to circumvent account lockout policies. The attempts are typically systematic and can be broken into two categories:

- **Dictionary attacks** start with a list of common words that may be used to form passwords. The words may be combined, broken down or sent through a variety of "morphing" algorithms to improve effectiveness.
- **Brute force attacks** walk through all the possible character combinations. First "AAAA1" is tried, then "AAAA2", then "AAAA3", and so on. Once all the five character passwords have been tried, the search begins anew with six character passwords.

Password length significantly increases resistance to brute force attacks. A single extra character makes a large difference: even if passwords are case insensitive and alphanumeric, one extra password means the typical brute force attack will take 36 times as long (10 digits plus 26 letters) to complete.

In addition to password guessing attacks, some legacy Microsoft protocols suffer from a limitation which makes an eight character password particularly important. These protocols effectively break down passwords into seven character "chunks". This creates two significant vulnerabilities:

- First, passwords with seven or fewer characters are quickly identified.
- Second, since a fourteen character password effectively becomes two seven character passwords, it is actually only twice as secure as a seven character password.

In order to protect against the first vulnerability, the general consensus requires passwords to be eight characters or more.

Protection against the second vulnerability, however, can only be provided through the use of stronger authentication protocols. In particular, LAN Manager (LANMan) and NTLM authentication contains this limitation; however, NTLMv2 and Kerberos are not affected by this. See 3.2.1.47, which discuss how to require NTLMv2 or Kerberos authentication, and how to disable storage of LANMan password hashes.

2.1.2 Password Age

All passwords must be changed regularly to ensure they are known only by individuals authorized to use the account.

In addition to limiting user accounts to a single user, this also controls the use of "role" accounts. Role accounts typically may be shared among users for maintenance and troubleshooting, or they may be required for various system services and applications, and are assigned privileges based on their specific purpose. Over time, role account passwords become well-known and an easy route to access resources. Since the accounts are shared by multiple individuals, it becomes very difficult to assign accountability when they are misused. The local administrator and various service accounts are often overlooked, and may have stale passwords which are well known by support personnel.

The requirement to change passwords also provides a practical defense against brute force password attacks. Given the nature of the brute force attack, it will always succeed if there is enough time to eventually guess the password. On a typical computer, it may take weeks or even months to guess a long alphanumeric password. However, if the password expired and was changed since during this period, the attack will fail. Therefore the maximum password length is also driven by the capacity of the most common password crack software.

2.2 Minor Auditing and Account Policies Requirements

2.2.1 Audit Policy (minimums)

Audit Policy defines the significant events which a computer should log. The log entries, or events, perform two important roles: they provide a means for near-real-time monitoring of the system, and they allow investigation of actions which occurred in the past.

When considering system security, audit events will often identify unauthorized attempts to access resources. The events can be generated from interactive user sessions, or from automated system processes and services. Default installations of Windows XP have security event logging disabled.

Security event logging is easily enabled. From the Windows Start menu, select Settings | Control panel. Under “Administrative Tools”, select “Local Security Policy”. In the console windows that appears, navigate down the tree to Security Settings | Local Policies | Audit Policy. To make changes, double-click one of the items, select the appropriate settings in the dialog box that appears, and select “OK”. Settings will take affect when the Local Security Settings window is closed.

2.2.1.1 Audit Account Logon Events

Audit logon events track all attempts to access the workstation. These may come from a local interactive logon, a network logon, a batch process, or even a service. Failed account logon may show a trend for password attacks; successful logon events are important to identify which user was logged on to the workstation at a given time.

“Account Logon” events are generated from the use of domain accounts; this differs from “Logon Events” (2.2.1.4) which are generated by the use of local accounts.

2.2.1.2 Audit Account Management

In order to track successful and failed attempts to create new users or groups, rename users or groups, enable or disable users, or change accounts’ passwords, enable auditing for Account Management events. Successful account management events are also generated when an account is locked out, so these events become important in determining the cause of an account lockout.

2.2.1.3 Audit Directory Service Access

No auditing of Directory Service Access is required on Windows XP Professional because Directory Service Access can only be audited on Windows 2000 (or later) domain controllers.

2.2.1.4 Audit Logon Events

Similar to 2.2.1.1 above, Logon Events will identify which accounts are accessing resources on the workstation. These events are generated only when local machine credentials are used. Even if a workstation is domain member, it is still possible to log on to the workstation using a local account.

2.2.1.5 Audit Object Access

It is possible to track when specific users access specific files. This option only produces events when one or more objects are actively being audited.

In order to track user access to specific files or directories, navigate to the file or folder, edit the security properties for that object, and enable auditing the object.

2.2.1.6 Audit Policy Change

When the “Audit Policy Change” option is set, changes to User Rights, Audit Policies, or Trust Policies will produce events in the Security Event Log.

2.2.1.7 Audit Privilege Use

Auditing privilege use enables auditing for any operation that would require a user account to make use of extra privileges that it has already been assigned. If this is enabled, Events will be generated in the Security Event Log if a user or process attempts to bypass traverse checking, debug programs, create a token object, replace a process level token, or generate security audits.

If security credentials are used to backup or restore files or directories using the “Backup or Restore” user right, and if this setting is set, security events will be generated.

Privilege Use is used by all user accounts on a regular basis. If success and failure events are audited, there will be a great many events in the event log reflecting such use.

2.2.1.8 Audit Process Tracking

When this option is enabled, an event is generated each time an application or a user starts, stops, or otherwise changes a process. This creates a very large event log very quickly, and the information is not normally exceptionally useful, unless you are tracking a very specific behavior. As such, auditing process tracking is not required, and is only recommended when absolutely necessary.

2.2.1.9 Audit System Events

Auditing System events is very important. System events include starting or shutting down the computer, full event logs, or other security related events that have impact across the entire system. Auditing of Success and Failure events should be enabled.

2.2.2 Account Policy

When applying the settings below, it is important to consider exactly where these settings must be applied to affect different account types:

- If the workstation is not a member of a domain, these policies can be applied locally and will be consistently applied to all local accounts.
- If the workstation belongs to a domain, any settings applied here will not impact domain accounts. In fact, the **account policy for domain accounts can only**

specified in the default domain policy. The account used by the workstation to log on to the domain is a domain account.

- If the workstation belongs to a domain, and is placed in a specific Organizational Unit (OU), machine account policy can be placed on that OU. The OU policy will apply to all local accounts on the workstation, and will override the local security policy.

See Microsoft Knowledge Base Article 255550 for more information.

2.2.2.1 Minimum Password Age

The recommended password policy requires users to change passwords regularly, and requires the password to be different from those cached in history. When the minimum password age is set to 0, a user can change passwords repeatedly. It is possible for the user to continue changing passwords until yesterday's password is flushed from the cache, and then re-use the old password. This activity is prevented by limiting password changes to once a day.

2.2.2.2 Maximum Password Age

See section 2.1.2 for a discussion on Maximum Password Age.

Maximum and minimum password age requirements are enforced by the logon process. If an account never logs off, it will continue to gain access to resources until the system reboots.

2.2.2.3 Minimum Password Length

See section 2.1.1 for a discussion in Minimum Password Length.

2.2.2.4 Password Complexity

Section 2.1.2 introduced the brute force password attack. Complex passwords further mitigate the risk of a brute force password attack by significantly increasing the set of all possible passwords. This is done by requiring passwords to include a combination of upper and lowercase letters, numbers and symbols (special characters) in the password.

Windows XP does not provide any granularity in password complexity requirements—it is either on or off. When complex passwords are required, each password must contain characters from three of the following four sets of characters:

- Uppercase letters
- Lowercase letters
- Numbers
- Special characters (non alphanumeric symbols)

Enabling this setting provides outstanding resistance to brute force password attacks, and should be set whenever possible, but may occasionally be difficult to implement. End-user education is a must, as the warning messages for weak passwords are cryptic and likely to be of little help to most users. Also, consider the impact to other non-Microsoft systems which integrate with the Microsoft authentication scheme, and make sure they support complex passwords as well.

If you are unable to require complex passwords, consider lengthening the minimum password length. Often a long alphabetic passphrase can be more resistant to a brute force attack than a short complex passphrase.

2.2.2.5 Password History

Passwords should be changed on a regular basis. By that same rule, users should not be permitted to use the same few passwords over and over again. The Enforce Password History setting determines how many previous passwords are stored to ensure that users do NOT cycle through regular passwords. The NSA requirement of 24 passwords remembered should be viable for public use as well.

When determining your overall account configuration, consider the combined effect of password history and maximum password age settings, and prevent repetitive patterns. For example, if your password age is 30 days and password history is 12 or less, many users will likely to set passwords to a variation of the current month (January1, February1, etc.).

2.2.2.6 Store Passwords using Reversible Encryption

The Windows authentication model allows storage of a password hash rather than the actual password. A password hash can not be decoded to regain the original password. Rather, to authenticate, the password must be hashed exactly the same way and compared with the original stored hash. If the values match, the correct password was presented, and access is granted.

In order to support some applications and their authentication, Microsoft permits the ability to store passwords using reversible encryption. If at all possible, this should be avoided. This option is disabled by default, and should remain so. Any application that requires reversible encryption for passwords is purposely putting systems at risk.

2.2.3 Account Lockout Policy

Many of the settings above protect against brute force and dictionary password attacks. Typically these attacks gather information (such as password hashes) and perform the attack offline. However, some password guessing attacks still occur interactively.

In order to protect against online password attacks, enforce an account lockout policy. Three settings comprise the account lockout policy: duration, threshold and reset.

2.2.3.1 Account Lockout Duration

Once the criteria for a lockout are met, the account becomes locked. However, the account will automatically become re-enabled once again after the duration specified in the “Account Lockout Duration.” Specify 0 minutes to have the account lockout until an administrator manually resets the account.

2.2.3.2 Account Lockout Threshold

The user is given a number of attempts to enter the wrong password before their account becomes locked. The “Account Lockout Threshold” defines this limit.

2.2.3.3 Reset Account Lockout After

Following a bad logon, the system increments the count of invalid attempts for this account. This counter continues to increment until the lockout threshold is reached, or the counter is reset. The “Reset Account Lockout After” setting defines how often the counter is reset. This setting must be less than or equal to the “Account Lockout Duration”, 2.2.3.1.

2.2.4 Event Log Settings – Application, Security, and System Logs

All system events are collected into event logs. All Windows XP systems contain three sets of logs: Application, System and Security. Application logs entries typically come from installed software; for example, anti-virus software will cut an event when virus scans complete, or when it detects a virus. The System log collects events generated by the operating system, such as system reboots and a startup or shutdown of event logs. The security log collects security audit information as defined by group policy. All three logs may contain useful information about a security incident.

The default size of each event log is 512k. This has been standard since the days of Windows NT 3.5, when hard drives were typically under 2 Gigabytes (GB) in size. However, recent hardware capacity improvements should leave ample storage space for an 80Mb event log.

Two additional settings control system behavior when the event log is full. Essentially there are two possibilities:

- Continue logging events as they come but risk overwriting important events
- Stop logging events

Obviously, it is preferable to continue logging events so that useful information is not lost. However, consider the attacker that kicks off a fake event generator as the last step of the attack (for example, it might try to log in with the guest account hundreds of times a second knowing the guest account is disabled). If all events continue to be logged, the events from the actual attack will soon be overwritten. In this case, it would be preferable to stop logging events when the log fills.

The Audit policy setting for “Log Retention Method” provides control over how the system reacts to a full log:

- **Overwrite Events as Needed** continues logging all events, overwriting older event whenever necessary.
- **Overwrite by Days** allows overwriting some events, but not all. Events older that a specific number of days can be cleared out. Once all the older events are overwritten, no new events are logged.
- **Do not overwrite (Clear logs manually)** prevents overwriting events, and new events are lost when the event log fills. The event log must be cleared manually by the system administrator or an automated log management application.

Setting the “Log Retention Method” to “Overwrite by Days” enables the “Log Retention” option. This specifies the number of days of event logs the system will preserve.

It may seem advisable to make the event logs as large as possible. However, due to constraints in how the operating system handles the logs, all three log files must be mapped to memory during normal system operation. An excessively large setting may cause unexpected results as the logs grow beyond the ability for the operating system to load the file in memory. Therefore, this guide recommended combined size of all three log files is limited to 120Mb, although a combined size of up to 300Mb seems to work well. A Microsoft Knowledgebase article describing this behavior was under development at the time this document was published.

2.2.4.1 Application Log

2.2.4.1.1 Maximum Event Log Size

2.2.4.1.2 Restrict Guest Access to Logs

2.2.4.1.3 Log Retention Method

2.2.4.1.4 Log Retention

2.2.4.2 Security Log

2.2.4.2.1 Maximum Event Log Size
2.2.4.2.2 Restrict Guest Access to Logs
2.2.4.2.3 Log Retention Method: **If set to "Do Not Overwrite," see 3.2.1.8**
2.2.4.2.4 Log Retention

2.2.4.3 System Log

2.2.4.3.1 Maximum Event Log Size
2.2.4.3.2 Restrict Guest Access to Logs
2.2.4.3.3 Log Retention Method
2.2.4.3.4 Log Retention

3 Security Settings

Security settings outline many very specific options which can improve a system's security by protecting against a specific threat.

To edit security settings, select Start | Settings | Control Panel. Double-click "Administrative Tools," and select "Local Security Policy". In the window that appears, expand Local Policies, and click Security Options. To make changes, double-click one of the settings in the right pane, make the appropriate changes, and click OK to save the settings.

If the workstation is not a member of a domain, the change will become effective immediately, even though it won't show up in the Local Security Policy editor until it is closed. If the workstation belongs to a domain, local changes will only become effective domain policy does not override the settings.

3.1 Major Security Settings

Microsoft operating systems typically support a legacy anonymous login known as a "null session". The null session is actually a login session where both the user id and the password are blank. Although the operating system places many restrictions on a null session, and it can never be used for an interactive logon, it may still be possible to gather significant information through this special anonymous account.

Null sessions can usually be safely disabled since they are a legacy feature. However, some legacy applications may cease to function properly after disabling null sessions, so testing is a must. The settings below outline controls available within Windows XP to limit exactly what information can be obtained through the null session. Note that these settings affect local workstation accounts and resources only, but not domain accounts and shares.

Note that Windows 2000 manages this setting differently, although the net effect remains the same. In Windows 2000, these options correspond to "Additional Restrictions for Anonymous Connections." Other minor differences in Windows 2000 and Windows XP policies as well, and Windows 2000 tools should not be used when setting policy for Windows XP machines.

3.1.1 Network Access: Allow anonymous SID/Name translation

Each object within Active Directory obtains a unique binary security identifier (SID). The operating system controls access to resources by their SID. SID formatting is well known, and some SIDs (e.g., local administrator and local guest) have properties which divulge the actual purpose of the account.

Disable this option to prevent the null user from translating the binary SID into the actual account name.

3.1.2 Network Access: Do not allow anonymous enumeration of SAM accounts

By default, the null session login can list all the accounts within its domain. This presents a significant security risk, particularly if strong passwords are not required. Should an attacker be able to anonymously gather all available accounts, they can then try some basic guessing to quickly locate accounts with blank or very weak passwords.

SAM stands for the Security Account Manager. The SAM database holds all account information including passwords, access rights and special privileges. Local account information resides in the local SAM database, a file on the workstation. Domain account information resides in the SAM database on the domain controller.

Beware of the syntax for this option: Enabled means only truly authenticated logins may enumerate other accounts; Disabled means all accounts can be gathered through the null session.

3.1.3 Network Access: Do not allow anonymous enumeration of SAM accounts and shares

See 3.1.2 above. In addition to protecting the list of user accounts, it also controls the list of network file shares established on the workstation. Documentation does not describe behavior if this setting conflicts with 3.1.2; however, if this setting is enabled, 3.1.2 should be enabled as well.

Beware of the syntax for this option: Enabled means only truly authenticated logins may enumerate accounts and shares; Disabled means all accounts and file shares can be gathered through the null session.

3.1.4 Data Execution Protection (SP 2 only)

Data Execution Protection (DEP) provides protection against buffer overflow attacks. The protection is implemented through either hardware or software, depending on the system configuration. By default, data execution protection is enabled for all applications compiled with specific options to protect against buffer overflows.

DEP can be disabled system-wide, or for specific applications. In fact, Microsoft also offers recommendations on how to deploy specific DEP settings through scripts. However, the most common way to access DEP settings is through the control panel. Select the “System” icon, and under the Advanced tab select Performance -> Settings. In the window that opens, click the Data Execution Prevention tab. In this window, you can disable DEP completely, or turn it on for specific applications only. Different options are available if your system supports hardware-based DEP.

Because of the significance of buffer overflow attacks, and because applications have to be specifically compiled to enforce software-based DEP, it is a major security requirement to enable DEP for all applications.

3.2 Minor Security Settings

3.2.1 Security Options

3.2.1.1 Accounts: Administrator Account Status

Each Windows XP installation creates an “Administrator” account that has the highest access to the system. The account has the highest possible access and can bypass most security controls local to the machine; it is comparable to the “root” account in Unix. Many system maintenance features require use of the Administrator account. However, in some environments, the existence of this account can present a security risk. By setting the "Administrator Account Status" to disabled, the account becomes unavailable.

Regardless of this setting, the administrator account remains enabled when booting in "safe mode."

3.2.1.2 Accounts: Guest Account Status

The Guest account can provide some regulation to unauthenticated users. Disabling this account will prevent unknown users being authenticated as Guests. This default installation disables this account, and it should remain disabled. is disabled by default, and should remain so.

3.2.1.3 Accounts: Limit local account use of blank passwords to console logon only

Windows divides computer logons into two main types: console or local logons and remote logons. In a console logon, the physically logs on to the device with the attached keyboard. Remote logons are performed across the network using various protocols such as telnet, FTP and remote desktop.

When this setting is enabled, the computer refuses remote logons if the user attempts to use a blank password, even if the blank password is valid for that account. Passwords should never be left blank.

3.2.1.4 Accounts: Rename Administrator Account

See 3.2.1.1. Often disabling the Administrator account is not practical. However, simply knowing the name of an account on a machine can be valuable information to an attacker. In an attempt to hide the account, best practices recommend renaming the account to something unique for your implementation.

If the account is renamed, anonymous Security Identifier (SID) / Name translation should also be disabled (3.1.1). This prevents an attacker from locating the renamed account by its SID.

3.2.1.5 Accounts: Rename Guest Account

See 3.2.1.2. Similar to the Administrator account, the Guest account should be renamed even if it is disabled. The operating system places additional safeguards on the Guest account, and it is less of a target than the Administrator account, but it still deserves significant attention warrant changing the account name.

3.2.1.6 Audit: Audit the access of global system objects

Global system objects typically only provide interesting audit information to developers. Some examples of these kernel objects include mutexes, semaphores and DOS devices. Normal system operation does not require auditing to this level of detail.

"Audit Object Access (2.2.1.5)" must be enabled before this setting will generate log entries.

3.2.1.7 Audit: Audit the use of backup and restore privilege

When enabled, this setting will generate a log entry for every file which is backed up or restored using the "Backup or Restore" privilege. During normal operations, this will generate a large amount of event entries, and is typically not required.

Various attacks are possible using backup or restore privileges. For example, an attacker may back up sensitive information to an unauthorized location. Or, the attacker may restore an invalid file—possibly a hacktool—from a tampered backup tape. In circumstances where the risk of improper backups and restores exists, this option should be considered. However, event logs must be sized appropriately (see 2.2.4).

"Audit Privilege Use (2.2.1.7)" must be enabled before this setting will generate log entries.

3.2.1.8 Audit: Shut Down system immediately if unable to log security alerts

See 2.2.4. A system administrator may choose not to overwrite events when the event log is full. Assuming that logs are sized appropriately, routinely backed up and cleared, this could indicate a security incident. In the specialized security environment, the inability to log events may be just cause to halt the server.

If the server is unable to log events and this setting is enabled, a Stop error occurs. To recover, the local Administrator must log on to the computer and manually clear the event log or change this setting.

Security Log Retention Method (2.2.4.2.3) must be set to "Do Not Overwrite Events" or "Overwrite Events by Days" for this setting to be effective.

3.2.1.9 DCOM: Machine Access Restrictions (SP2 only)

With Service Pack 2 for Windows XP, Microsoft introduced significant changes in the Distributed Component Object Model (DCOM) security model. DCOM provides computing services on non-standard TCP ports which can be accessed locally or remotely. These new restrictions are important in protecting against DCOM exploits. Since many services can be published through the DCOM interface, the machine administrator retains little or no control over authentication settings. The new options allow the administrator to place system-wide restrictions on all DCOM services: All DCOM requests must first be authenticated, and then the provided credentials are matched against this ACL to determine if access is granted. Note that many DCOM applications will provide more granular security controls for a specific published service.

With this setting, you can define the accounts that are allowed to access existing DCOM services. The default setting allows anonymous access to access DCOM services from the local machine only, but everyone is allowed remote access.

The setting is specified in Security Descriptor Definition Language (SDDL). Although you can define this manually, it is often best to use the Group Policy Editor interface to create the SDDL string.

3.2.1.10 DCOM: Machine Launch Restrictions (SP2 only)

Additional restrictions can be placed on which accounts are allowed to activate or launch DCOM services. Launch permissions are required to start a COM server when it is activated. Activation is the process of getting a COM interface proxy, and sometimes requires the COM server to be launched.

By default, only administrators can remotely activate or launch DCOM service. The "everyone" group is allowed to launch or activate only from the local machine.

3.2.1.11 Devices: Allow undock without having to log on

Can't a laptop always be undocked simply by lifting it off the dock? Surprisingly, the answer is no. Some laptop docking stations have a hardware eject button that can actually be locked by software on the laptop. Setting this option to disabled provides greater security; however, without proper training a user may physically damage the hardware.

Beware of the syntax for this option: Disabled means a user must log in to the laptop and request to undock it; Enabled means the laptop can be unlocked at any time

3.2.1.12 Devices: Allowed to format and eject removable media

This setting governs the type of users which have authority to remove NTFS formatted media from the computer. The available choices (listed from most to least restrictive) are Administrators, Administrators and Power Users, or Administrators and Interactive Users.

3.2.1.13 Devices: Prevent users from installing printer drivers

Users typically need the ability to install and configure their own printers. However, printer driver installation loads code directly into the privileged space of the operating system kernel. The malicious user could choose to install an invalid or trojaned print driver to gain control on the system.

Preventing users from installing printer drivers may lead to unwanted support calls. If users must be given the right to install printer drivers, consider requiring that the driver be digitally signed before it can be installed (see 3.2.1.14).

Beware of the syntax for this option: Enabled means the users will not be able to install printer drivers and may prevent proper setup of printers; Disabled allows the user to fully manage their own printers.

3.2.1.14 Restrict CD-ROM Access to Locally Logged-On User Only

With sufficient privileges, users can create network shares from any folder on a Windows XP workstation. This extends to sharing a CD-ROM drive externally. This setting would restrict use of the shared CD-ROM drive to the local interactive logon. Since different CDs can be inserted, the user may forget or be unaware that the information on the CD becomes remotely accessible. Also, unlike typical file shares, access control lists can not be placed on files and directories to control access and auditing.

Generally, users and processes should not need to remotely access a workstation CD-ROM drive; however, enabling this setting could cause problems with some software installation packages. When users install software from a CD-ROM drive, and the installation package uses the Microsoft Installer (.msi packages), the Windows Installer service actually performs the installation. The install will fail, since the service account does not If this setting is enabled, such software installation will not be able to proceed, because of this restriction. The setting must be changed long enough to install the software, or the package must be copied to a local or network drive for the installation procedure to succeed.

Beware of the syntax for this option: Enabled means users will **not** be able to access CD-ROM shares. Disabled allows access to shared CD-ROMs (share-level access permissions still apply).

3.2.1.15 Devices: Restrict Floppy Access to Locally Logged-On User Only

Similar to a CD-ROM drive (3.2.1.12 above), the floppy drive can be shared to network users. Again, the user may not remember that the information on all inserted floppies becomes exposed.

Beware of the syntax for this option: Enabled means users will **not** be able to access shared floppy drives. Disabled allows access to shared floppy drives, but share-level access permissions still apply.

3.2.1.16 Devices: Unsigned Driver Installation Behavior

Drivers interact with the kernel and hardware at a low level; improper drivers can open the system to low level hardware and kernel problems. Additionally, trojaned drivers can open the system to compromise. Microsoft generally ships drivers with a digital signature, expressing that Microsoft itself has certified the drivers through their Windows Hardware Quality Lab. Unfortunately, not all drivers (even from Microsoft) have digital signatures.

Options for this setting are "Silently succeed," "Warn but allow installation," and "Do not allow installation." The user should be notified if drivers are not signed; however, some end-user training may be required. However, the "Silently succeed" option may be required in managed environments where unattended software installations are commonplace.

3.2.1.17 Domain Controller: Allow Server Operators to Schedule Tasks

This setting applies only to Windows 2000 Server Domain Controllers. It has no effect on Windows XP workstations.

3.2.1.18 Domain Controller: LDAP Server Signing Requirements

This setting is not currently enforced, and must be set at the LDAP server (domain controller). This setting is disabled on Windows XP workstations, which has the same effect as "None": data signing can optionally be negotiated by the client and server.

3.2.1.19 Domain Controller: Refuse machine account password changes

This setting only applies to domain controllers. See 3.2.1.21 for the corresponding client workstation setting.

3.2.1.20 Domain Member: Digitally Encrypt or Sign Secure Channel Data (Always)

When a domain workstation boots up, it creates an encrypted tunnel with a domain controller to pass sensitive information. For example, management of the workstation's computer account password, user account password changes, and the exchange of private keys with Active Directory all occur through this NetLogon secure RPC channel.

With this setting enabled, all packets sent from the client will be signed. The client will also encrypt the packets if the server supports it. A signed packet can not be spoofed or tampered; however, the payload remains untouched and could possibly be deciphered should it be intercepted. Encrypted packets can only be decrypted by the server.

This setting can only be safely enabled when all domain controllers are Windows 2000, or Windows NT SP 4 or later.

3.2.1.21 Domain Member: Digitally Encrypt Secure Channel Data (When Possible)

See 3.2.1.18 above. This setting provides greater compatibility than requiring encryption or signing.

3.2.1.22 Domain Member: Digitally Sign Secure Channel Data (When Possible)

See 3.2.1.18 above. This setting also provides compatibility with legacy equipment. It prevents replay and man-in-the middle attacks when domain controllers support signing. However, by itself, this setting will not protect against packet sniffing to gather potentially sensitive information.

3.2.1.23 Domain Member: Disable Machine Account Password Changes

If a computer is a member of a domain, it has an account within the domain. During the boot up process, the computer logs in to the domain and establishes a secure channel for the exchange of sensitive information (see 3.2.1.18). Although the account can not be used for interactive logons, it can be used to authenticate to domain resources. This setting only impacts workstations which have joined a domain.

Like any other account, the computer account has a name and password. The computer manages its own password and changes it to a strong password regularly. This setting can be used to prevent the machine from managing its own password. Should the machine's local copy of the password falls out of synch with the domain controller's copy, the machine can not access domain resources, and the machine must be re-joined to the domain.

Beware of the syntax for this option: Disabled means the workstation will change its password; Enabled means workstation passwords are never changed.

3.2.1.24 Domain Member: Maximum Machine Account Password Age

See 3.2.1.21 above. This setting determines how often the computer resets its password. Remember that machine password changes do not visibly impact the end user, and they should be consistent with corporate policy for account management.

3.2.1.25 Domain Member: Require Strong (Windows 2000 or later) Session Key

This setting applies specifically to the NetLogon secure channel established between workstations and domain controllers (see 3.2.1.18). This setting only impacts workstations which have joined a domain.

By default, workstations will accept a weak 64-bit session key to encrypt the secure channel. However, this setting allows the workstation to require a strong 128-bit session key for the secure channel.

Only enable this setting if all domain controllers support a 128-bit encrypted secure channel. This is not supported on NT4 domain controllers; Windows 2000 domain controllers require Service Pack 2 or later.

This option is enabled by default, and it should remain so.

3.2.1.26 Interactive Logon: Do Not Display Last User Name

Anyone attempting to log into a computer may see the name of the last valid user who logged on to that system. This does not prevent displaying the currently logged on user when unlocking a workstation. This information may seem trivial, but it helps an attacker tie a workstation to a particular individual, or may help an attacker gain access to a stolen mobile device.

Educate users before enabling this setting in a domain environment. Some users may not know their logon, particularly when it differs from the e-mail address or other accounts.

Beware of the syntax for this option: Enabled means the user must type in their user id on every logon; Disabled means the last logged on user appears in the login dialog.

3.2.1.27 Interactive Logon: Do not require CTRL+ALT+DEL

The Windows operating system treats the CTRL+ALT+Delete key different from any other. Operating system design prevents any application from intercepting and responding when these keys are pressed. When you type CTRL+ALT+Delete, you are guaranteed that the operating system authentication process will handle the request.

With the CTRL+ALT+Delete requirement lifted, the user could actually be typing their password into a trojaned application, rather than the operating system authentication process. Remember, the trojaned application would not be able to respond had the user pressed CTRL+ALT+Delete.

When a workstation does not require CTRL+ALT+Delete to log on, users will not see the dialog "Press CTRL+ALT+Delete To Log On." Rather, the workstation simply presents the standard logon dialog.

Beware of the syntax for this option: Disabled means the user must press CTRL+ALT+Delete before every non-smartcard logon; Enabled will present the logon dialog without requiring CTRL+ALT+Delete.

3.2.1.28 Interactive Logon: Message Text for Users Attempting to Log On

In general, legal requirements dictate that users must be notified of security practices when logging on to a system. The users should agree to acceptable usage policies, and be notified that the system may be monitored. The message is commonly referred to as a "logon banner".

The sample banner provided below has been approved by the United States Department of Justice. The United States government deems it suitable for use. For corporate networks and workstations, defer the actual text to your legal counsel, perhaps using this message as a template.

> This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel. In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.

3.2.1.29 Interactive Logon: Message Title for Users Attempting to Log On

The message title acts as part of the logon banner discussed above. The workstation places this text as the title for the logon banner window. The text should be either neutral or a warning. Avoid inviting titles such as "Welcome".

3.2.1.30 Interactive Logon: Number of Previous Logons to Cache

When a workstation belongs to a domain, users can log on to it using domain credentials. The domain credentials can be cached in the local workstation's Security Accounts Manager (SAM) database. On next logon, should no domain controller be available, the user can still log on locally by authenticating against the cached account information.

When logging on using cached credentials, some account properties will not be enforced, since the domain controller maintains responsibility for enforcing account policy. The local SAM database does not "own" the account, so cached account passwords do not expire, and domain accounts can not be locked out when the domain is unavailable.

When establishing corporate policy for cached accounts, consider the remote user. They commonly log on with cached credentials from a laptop. To access corporate resources, the user establishes a Virtual Private Network (VPN) connection to the corporate network. Since logon occurs before the domain is available—the VPN has not yet been established—the user will never be prompted to change the password on the cached account.

This setting only affects workstations joined to a domain, and only impacts interactive logons with domain accounts. The workstation will not cache non-interactive log on information. Change this setting to zero to disable the caching of domain accounts in the local SAM database.

3.2.1.31 Interactive Logon: Prompt User to Change Password Before Expiration

Should a user's password be near its expiration date, the logon process warns the user and asks if they would like to change the password. Once the password has expired, the user will be required to change the password to complete the logon. This setting governs the window of convenience between the time when the system offers the user to change the password, and the time when they are required to change the password.

3.2.1.32 Interactive Logon: Require Domain Controller authentication to unlock workstation

This setting results from a feature in Windows domain authentication; a further understanding of the behavior will help you determine the setting applicable to your organization. This setting does not affect standalone workstations.

The typical sequence for failure to unlock a workstation flows something like this:

1. The user repeatedly types in the wrong password.
2. For each password attempted, the workstation first compares the password to the cached password hash used for the original logon. If they do not match, it contacts the domain controller and attempts to log on.
3. After a predefined number of attempts, the domain controller locks out the account, and the workstation reports the account lockout.

At this point, most users will contact the system administrator and have the account lockout and perhaps the password reset. However, consider the persistent user that continues attempting to logon:

4. The user continues attempting to logon. Each time a bad password is entered, the workstation still compares it to the local cache; when the comparison fails, it contacts the domain controller, which also denies the logon.
5. Finally, the user enters the correct password. The workstation comparison to the local cache succeeds.

If this setting is disabled, the user then successfully unlocks the workstation. Even with a locked account, the user can then continue to access network resources for connections which were established and authenticated before the machine was locked—mail servers and file servers in particular.

Enabling this setting, however, adds an additional step after every successful workstation comparison with the local cache:

6. The workstation presents the credentials to the domain controller. Only if the domain controller authentication succeeds will the workstation be unlocked.

Enabling this setting to protect against brute force password attacks through the screen saver. However, enabling it will hinder the user who locks and hibernates their workstation, and then attempts to resume when the domain controller is unavailable. Disabling this setting (or leaving it undefined) minimizes domain controller traffic.

For more information, see Microsoft Knowledge Base Articles 188700, "Screensaver Password Works Even If Account Is Locked Out" and 281250, "Information About Unlocking a Workstation"

3.2.1.33 Interactive Logon: Smart Card Removal Behavior

When users authenticate with smart cards, the system can be set to lock or log out the user when the smart card is removed. Any setting other than "No Action" is acceptable.

In an environment that does not use Smart Cards, this setting has no effect.

3.2.1.34 Microsoft Network Client: Digitally sign communications (always)

This setting applies specifically to communications using the Server Message Block (SMB) protocol. When enabled, the client will negotiate signed communications with any SMB server. If the server can not support SMB signing (typically servers prior to Windows 2000), communications will fail.

When possible, digitally sign client communication to protect against man-in-the-middle attacks, as it supports mutual authentication and protection against packet tampering.

SMB signing does not impact network bandwidth; however, CPU resources will be used in generating and verifying SMB signatures.

3.2.1.35 Microsoft Network Client: Digitally sign communications (if server agrees)

This setting applies specifically to communications using the Server Message Block (SMB) protocol. When enabled, the client will negotiate signed communications with any server supporting SMB signing (typically Windows 2000 and later). Unsigned communications will still succeed with servers that do not support message signing.

3.2.1.36 Microsoft Network Client: Send Unencrypted Password to Connect to Third-Party SMB Server

Would you like your Windows XP computer to send your password in clear text to another computer that requests authentication? The setting is disabled by default, and should remain so.

If you find an application that requires this setting to be enabled, please first send feedback to windows-feedback@cisecurity.org so we can document it and contact the manufacturer. We will request a product redesign with better security, which will not require this behavior.

3.2.1.37 Microsoft Network Server: Amount of Idle Time Required Before Disconnecting Session

This setting applies specifically to communications using the SMB protocol. When a client establishes a connection with an SMB server, they exchange credentials, perform authentication, and set aside resources to manage the connection. After a period of inactivity, the client or server may close the connection to conserve resources. When the client again attempts to use the SMB server, it reestablishes the connection without interaction with the user. The reconnection typically happens fast enough to hide the activity from the user.

Computers that do not share resources with other Windows computers are not affected by this setting.

3.2.1.38 Microsoft Network Server: Digitally sign communications (always)

Similar to 3.2.1.32, the workstation may require all SMB traffic to be digitally signed. Workstations act as servers when remote devices connect to published shares; many workstation management systems also use SMB protocols.

This setting will likely have less impact to the workstation than 3.2.1.32, since remote connections to workstations are typically well understood.

3.2.1.39 Microsoft Network Server: Digitally sign communications (if client agrees)

Similar to 3.2.1.33, the workstation should request signed communications wherever possible. This option is enabled by default, and should remain enabled.

3.2.1.40 Microsoft Network Server: Disconnect clients when logon hours expire

This setting only applies to workstations joined to a domain, as logon hours can not be set for local accounts. Additionally, this applies only to network connections established with the SMB protocol.

Domain accounts may be limited to specific hours when they may be used. By default, the domain controller only enforces these settings upon logon, but not after the session is established. With this setting enabled, should a user remotely log in to this workstation (the workstation acts as a server), the user's network connections will be closed when their allotted time has been reached.

3.2.1.41 Network Access: Do not allow storage of credentials or .NET passports for network authentication

This setting controls behavior of the "Stored User Names and Passwords" feature of Windows XP. This feature stores NTLM, Kerberos, Passport and SSL authentication; it should not be confused with the Internet Explorer authentication cache, since it is managed separately. Some documents refer to this setting as "Network Access: Do not allow Stored User Names and Passwords to safe passwords or credentials for domain authentication".

Beware of the syntax for this option: Enabled keeps credentials out of the cache; Disabled allows storing user names and passwords.

3.2.1.42 Network Access: Let Everyone permissions apply to anonymous users

Many resources across the network are accessible to the "Everyone" group. This special group contains all accounts; however, it does not contain the anonymous user (null session, see section 3.1). Enabling this option adds the "null user" to the "Everyone" group, escalating privileges of this account. The "Everyone" group is assigned to many network resources by default.

This option is disabled by default and should remain disabled.

3.2.1.43 Network Access: Named pipes that can be accessed anonymously

Named Pipes are communications channels between two processes. The process may or may not be located on the same computer, and communications are peer-to-peer rather than client-to-server. Each pipe is assigned an access control list.

This setting defines which pipes can be accessed remotely without authentication, and should be left blank.

3.2.1.44 Network Access: Remotely accessible registry paths

This setting defines the registry paths which can be accessed from another computer. Remote registry access depends on the remote registry service and requires authentication.

3.2.1.45 Network Access: Shares that can be accessed anonymously

Access Control Lists restrict access to published network shares hosted by a workstation. Shares can be published to the "Everyone" group, but this does not include the unauthenticated null user. Adding specific shares to this list grants access to the unauthenticated user. Note that NTFS permissions on the share still apply.

3.2.1.46 Network Access: Sharing and security model for local accounts

Remote users often must present logon credentials to the workstation to gain access. Occasionally, they may present credentials for a local account on the workstation. In the

"Classic" security model, even though a remote user is using local credentials, they still gain access based on restrictions for the local account. However, the "Guest Only" model remaps the remote user to the guest account, so they will only be able to access resources available to guests.

3.2.1.47 Network Security: Do not store LAN Manager password hash value on next password change

The SAM database typically stores a LANManager (LM) hash of account passwords. The SAM database should be secure on the workstation; however, if it is captured, the LM hash can be retrieved. Many vulnerabilities exist with the LM authentication model, and brute force attacks usually succeed with ease. Removing the LM hash from the SAM database helps protect the local account passwords. However, most Windows 9x clients only support LM authentication.

Beware of the syntax for this option: Enable this setting to keep the password secure; Disable this setting to weaken the password database and allow Windows 9x clients to log in remotely to the workstation.

3.2.1.48 Network Security: Force logoff when logon hours expire

This setting is similar to 3.2.1.38, but reflects the client-side settings. This setting only applies to workstations joined to a domain, as logon hours can not be set for local accounts. The setting deals exclusively with connections using the SMB protocol, and not with the interactive logon session.

Enabling this feature will disconnect all client connections when logon time limits are reached. By default, the workstation only enforces logon hours during session setup, and not afterwards.

3.2.1.49 Network Security: LAN Manager Authentication Level

Windows network authentication has changed considerably as various security vulnerabilities have been identified and fixed. The original LAN Manager (or LM) password hash is considered very weak, but is still used by most Windows 9x clients. Using commercially available software, and off-the-shelf computers, most LM password hashes can be used to reveal the actual password in a matter of days, or hours.

With the release of Windows NT 4.0, Microsoft developed NTLM authentication. Serious vulnerabilities made NTLM almost as easy to crack as LM, so NTLM version 2 (NTLMv2) was introduced. NTLMv2 provides significant improvements to security; when combined with strong password policy, accounts are well protected against brute force attacks. All of these authentication methods are incorporated into Windows 2000.

All authentication models work with a hash of the password, not the password itself. This presents challenges with down-level compatibility between operating systems. In order to smooth the transition, when one computer attempts to authenticate with another, the default behavior is to send the basic LM hash along with the more secure NTLM hash. This setting improves control over the response to an authentication challenge:

Send LM & NTLM responses
Send LM & NTLM, Use NTLMv2 session security if negotiated
Send NTLM response only
Send NTLMv2 response only
Send NTLMv2 response only\refuse LM
Send NTLMv2 response only\refuse LM & NTLM

The default, and weakest option, is the first: send LM & NTLM responses. As a result, using NTLM is ineffective because both protocols are sent together. In order to take a much more effective stand to protect network authentication, set LAN Manager Authentication Level to "Send NTLMv2 response only\refuse LM & NTLM".

Enabling this setting may have adverse effects on your ability to communicate with other Windows machines unless the change is made network-wide. If you find that you are unable to require a certain level of LM Authentication, back down to "Send LM & NTLM – Use NTLMv2 session security if negotiated" and try your network authentication again. Communication with Windows 9x/Me machines requires the DSCLIENT.EXE utility from the Windows 2000 installation CD.

3.2.1.50 Network Security: LDAP client signing requirements

Similar to the SMB protocol, the LDAP protocol supports signing. LDAP, "Lightweight Directory Access Protocol," provides one means for the client to talk to active directory. LDAP protocol is text-based, but supports authentication to gain access to sensitive sections of the directory. Require signing to provide the assurance of mutual authentication for this communications channel.

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

NTLM authentication can provide a security service to manage connection between various clients and servers, including through the Remote Procedure Call (RPC) service. Windows 2000 improved the security model for secure, authenticated client-server communications; this setting manages the new features for communications established by this workstation.

3.2.1.52 Network Security: Minimum session security for NTLM SSP based (including secure RPC) servers

Similar to 3.2.1.49, this setting manages features for communication services provided by this workstation to other computers.

3.2.1.53 Recovery Console: Allow Automatic Administrative Logon

The Recovery Console, new to Windows 2000 and XP, provides a limited command-line access to an otherwise unbootable operating system.

The console allows access to the NTFS file system, which does not natively allow access when the operating system becomes unbootable. Other third-party applications have been developed to perform this action as well, but the Recovery Console is part of the operating system. It can be installed from the Windows 2000 CD with the "*d*:\i386\winnt32.exe /cmdcons" command. It can also be run directly from the Windows 2000 installation CD.

The Recovery Console does not grant full and unrestricted access to the operating system by default. It does require that you log on using the password of the default Administrator account. Keep in mind that this must be the local administrator account, not just a member of the local administrators group. Also, the policy for renaming the administrator account does not apply to the recovery console, and that password must be used.

If configured, a boot to the recovery console could result in automatic logon, and bypass the need for the password of the administrator account. Since this gives administrator access to anyone who can reboot the computer, the setting is generally disabled.

3.2.1.54 Recovery Console: Allow Floppy Copy and Access to All Drives and All Folders

By default, the Recovery Console only allows access to the root folder of each drive, and the operating system folder (typically C:\Windows). The console also prevents copying files from the hard drive onto removable media. Although this protection can be bypassed by enabling floppy copy and drive access, the setting is enabled by default and should remain disabled.

3.2.1.55 Shutdown: Allow System to be Shut Down Without Having to Log On

Some systems run critical processes and should only be shut down by authorized users. Occasionally, special processes could be evoked during system startup, sometimes even trojaned processes. In environments where abnormal system reboots could cause problems, require a logon prior to reboot.

3.2.1.56 Shutdown: Clear Virtual Memory Pagefile

Virtual memory extends the physical memory available to the CPU. As data and applications fill the available physical memory, the operating system writes less-frequently used pages of memory out to disk, into the virtual memory pagefile. This greatly extends the amount of "virtual" memory available to the computer.

Since the pagefile contains information that was in memory, it potentially holds a great deal of information useful for an attacker. Digging through the pagefile can reveal SSL web pages, queries set from the client to databases, sometimes even user ids and passwords from poorly written applications.

The workstation does not clean this information from the pagefile on shutdown. Although the file can not be accessed when booted in Windows, anyone booting the workstation to an alternate operating system (e.g., from a boot CD) may access the page file.

Enabling this options provides greater security by erasing the data during normal operations; however, this may also significantly increase the time required to shut down the computer. When enabled, the hibernation file (hiberfil.sys) is also cleaned on shutdown.

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

FIPS stands for "Federal Information Processing Standards". The National Institute of Standards and Technology (NIST) maintains the standards, available online at http://www.itl.nist.gov/fipspubs/index.htm. Although the operating system can support a variety of hashing and encryption algorithms, only the following are FIPS compliant:

- Secure Hash Algorithm (SHA-1) for hashing
- Triple Data Encryption Standard (DES) for encryption
- RSA for key exchange and authentication.

Only these algorithms are used when the workstation requires FIPS compliant algorithms. With this setting enabled, the encrypting file system (EFS) will use triple DES rather than the default DESX.

NOTE: Enabling the requirement for FIPS compliant system cryptography will limit the workstation's ability to interact with SSL encrypted web sites that do not support these encryption mechanisms. This will likely have an effect on most non-IIS served web sites.

3.2.1.58 System objects: Default owner for objects created by members of the Administrators group

When an Administrator creates an object (file, directory, account, or any object which obtains and ACL from the operating system), an owner will be assigned. Normally, the account which created the object is assigned as the owner; however, changing this option allows assignment to the "Administrators Group" rather than an individual account.

3.2.1.59 System objects: Require case insensitivity for non-Windows subsystems

The Windows operating systems ignore case when accessing resources; for example, "C:\Windows", "C:\WINDOWS" and "c:\windows" all refer to the same directory. However, the Windows kernel allows interfaces with other case-sensitive operating systems (e.g., Unix). Enabling this setting causes the interoperability features to be case-insensitive as well.

This setting has no effect when the workstation communicates only with other Windows systems.

3.2.1.60 System objects: Strengthen default permissions of internal system objects

This setting actually digs deep into the operating system behavior and should be left at the default setting (Enabled) unless explicitly required.

"Internal system objects" are shared physical and logical resources such as semaphores and DOS device name; the objects all are created with access control lists (ACLs). When enabled, the ACL allows other non-administrative system processes to query internal system objects, but will not allow them to modify them.

3.2.2 Additional Registry Settings

The following paragraphs describe individual security settings that can be applied in a variety of ways – using REGEDIT.EXE, REGEDT32.EXE, Local Group Policy, or Domain Group Policy. For more information on applying changes directly to a Windows XP Professional registry, please consult the Microsoft TechNet Internet site at http://www.microsoft.com/technet. Some other helpful registry information is available at http://support.microsoft.com/default.aspx?scid=kb;en-us;Q256986 and http://www.microsoft.com/technet/prodtechnol/winntas/tips/winntmag/inreg.asp.

WARNING: Editing the registry can make a system unbootable and unusable if done improperly. If you are not familiar with editing the registry, please take a few minutes and follow the links to Microsoft's TechNet resources, and learn about some of the precautions you should take before editing the registry.

3.2.2.1 Suppress Dr. Watson Crash Dumps

Dr. Watson is one of Microsoft's utilities that handles errors in applications. If an application produces an error that Dr. Watson can manage, it will dump the contents of memory for that application to a file for future analysis.

In the process of writing the contents of memory to disk, it is entirely possible that password information could be written to disk as well, and later exploited. Set this value to zero to prevent Dr. Watson from writing crash dumps to disk.

3.2.2.2 Disable Automatic Execution of the System Debugger

If an application is executed in non-privileged memory, and the system debugger is started, it is possible for that application to execute code in privileged memory space. Set this value to zero to prevent the system debugger from executing automatically.

3.2.2.3 Disable autoplay from any disk type, regardless of application

Although it is convenient for applications to automatically run when Windows Explorer opens up, it can also cause applications to be executed against the wishes of an administrative user, and exploiting that privilege. Set this value to 255 to prevent any type of drive from automatically launching an application from Windows Explorer.

3.2.2.4 Disable autoplay for the current user

Note: Due to the inability to manage registry entries for each local user via Security Templates, this setting is recommended, but not required or measured.

3.2.2.5 Disable autoplay for new users by default

Similar to the autoplay settings above, this enforces the policy for any new profiles created on the workstation.

3.2.2.6 Disable Automatic Logon

Windows also has the ability to automatically log a user on every time that machine starts up. Some users may prefer this as a feature. Some server based applications may require that a user log in before they can execute, so they require this activity as well.

The problem with this "feature" is that in order for it to work, it stores the username and password for that user in plaintext in the registry. Set this value to zero to prevent any user from automatically logging in when the computer starts up.

3.2.2.7 Disable automatic reboots after a Blue Screen of Death

If someone manages to get enough control of your computer that they can plant an application there, the next step is to force your computer to restart to register that app. One easy way to accomplish this task is to programmatically force an error that causes the computer to crash, or "Blue Screen" which will reboot the machine by default. Set this Value to zero to prevent this behavior from happening, and at least alert the user that something is wrong.

3.2.2.8 Disable CD Autorun

If malicious software is written to a CD, it can be executed by Windows Explorer just by putting the CD in the drive. Set this value to zero to prevent any applications from automatically launching from the CD-ROM drive.

3.2.2.9 Remove administrative shares on workstation (Professional)

Every Windows NT/2000 computer automatically has "Administrative Shares" installed by default. These are restricted to use by Administrators, but they expose each volume root, and the %systemroot% folder to the network as Admin$, C$, etc. These make remote administration convenient, but they also present a risk if someone manages to guess the password to an administrative account.

WARNING: If you use administrative shares on your network for remote backups, antivirus support, or general remote administration, this will break your applications. Please ask your software vendors to design around this requirement in future versions of their applications.

3.2.2.10 Protect against Computer Browser Spoofing Attacks

Although this standard advises end-users to shut down their Computer Browser service, it is also likely that not everyone will be able or willing to do so. This registry setting provides protection against a vulnerability that allows the Computer Browse to be shut down. Set this value, to protect against this specific vulnerability. If you are not running the Computer Browser service, this setting will have no effect. More information is available at http://support.microsoft.com/default.aspx?scid=kb;EN-US;q262694.

3.2.2.11 Protect against source-routing spoofing

If a Windows computer has two valid networking devices installed, it can be configured to act as a router or a firewall, and pass network traffic from one interface to another. Whether this is the intended purpose or not, it can be done on any Windows computer. "Source Routing" traffic that passes through such a router can bypass certain routing rules by "spoofing" the device to think malicious network activity came from the protected side. Set this value to 2 in order to drop all source routed packets.

3.2.2.12 Protect the Default Gateway network setting

When one TCP/IP Default Gateway fails, it is possible to force one computer to use a second default gateway to complete the route path. In most cases, computers are not set up with multiple default gateways, relying on redundant routers instead.

If an attacker can manipulate your default gateway, and this setting is not set to zero, he could route your network traffic to an alternate address. Set this value to zero to protect against this kind of attack.

3.2.2.13 Ensure ICMP Routing via shortest path first

In order to prevent network ICMP traffic from being redirected from one computer to another, set the EnableICMPRedirect value to zero. There is some confusion as to whether or not the value name is pluralized. For more information, please refer to the Microsoft article at http://support.microsoft.com/default.aspx?scid=kb;EN-US;q293626.

3.2.2.14 Help protect against packet fragmentation

When data is transferred across a network, the data is broken down into packets. These packets are not always a uniform size. When these packets are broken down into smaller sizes, they are supposed to be reassembled at the other end of a network route in the same order. This does not always go as planned, and can used in some network attacks.

Set this value to 0 to force Windows to use a consistent 576 byte packet. More details are available at http://support.microsoft.com/?kbid=315669.

3.2.2.15 Manage Keep-alive times

The KeepAliveTime determines how often the network subsystem attempts to verify that a TCP session is still active. The setting of 300,000 works out to one request every five minutes.

3.2.2.16 Protect Against Malicious Name-Release Attacks

By default, a computer running NetBIOS will release its name upon request. In order to protect against malicious name-release attacks, set this value to 1. Microsoft also references in at least one place that this is for Windows 2000 Service Pack 2 or greater.

3.2.2.17 Ensure Router Discovery is Disabled

This setting prohibits the workstation from caching router advertisements. Since router advertisements propagate through UDP, they can easily be spoofed.

3.2.2.18 Protect against SYN Flood attacks

One of the first methods of launching Denial of Service attacks was to send a flood of incomplete 3-way handshake requests. Each time the incomplete request was received by the target, a small portion of the target's resources were set aside, waiting for the request to finish. When all of the resources were set aside, the target machine was no longer able to serve any more requests, and further service was denied.

In order to prevent the success of this attack, set the SynAttackProtect value to 2, which allows the operating system to limit the amount of resources that are set aside until the 3-way handshake is completed. Setting SynAttackProtect to 1 provides minimal security, but for maximum protection, set it to 2.

The next few settings also provide a measure of protection against Denial of Service or Distributed Denial of Service attacks.

3.2.2.19 SYN Attack protection – Manage TCP Maximum half-open sockets

This value determines how many incomplete handshake requests the network will allow at one time. This provides protection if SynAttackProtect is set to 1. 100 is the default value on Windows XP Professional.

3.2.2.20 SYN Attack protection – Manage TCP Maximum half-open retired sockets

This value indicates how many retransmitted SYN sessions are permitted. The Default value is 80 for Windows XP Professional.

3.2.2.21 Enable IPSec to protect Kerberos RSVP Traffic

When Kerberos authentication information is transferred between domain controllers, or between domain controllers and member servers or workstations, it is not secured by default. Even when IPSec is used to encrypt that traffic, the Kerberos information is considered "exempt". Set this value to 1 to ensure that all traffic, including Kerberos information is protected by IPSec.

3.2.2.22 Hide workstation from Network Browser listing

If the Computer Browser service is disabled, or if this computer is not part of a domain, this setting has no effect. Otherwise, it will prevent the computer from announcing itself to the browser services of other computers, and only act as a "listener" on domain browse lists.

WARNING: This setting will remove your computer from the list of available computers in your domain in Network Neighborhood. This should already be done by disabling the Computer Browser service, but this setting will perform the same function.

3.2.2.23 Enable Safe DLL Search Mode

This setting modifies the way in which Windows locates driver files (.dlls). A value of 0 forces the operating system to search the current directory first; when set to 1, the system searches the windows system directory first.

3.2.2.24 Disable WebDAV basic authentication (SP 2 only)

The WebDAV (distributed authoring and versioning) service allows an XP client to manage documents using the HTTP protocol. Since documents can be modified, locked and deleted through this protocol, the server typically requires the client to authenticate, which is also done through the HTTP protocol.

The HTTP client and server must negotiate an acceptable authentication protocol. Valid options include Kerberos, NTLM and Basic authentication. Basic authentication is often the easiest to implement, but it requires transmitting the username and password over the network in clear text.

In order to prevent the WebDAV service from negotiating basic authentication, set this option to a non-zero value. If the registry key does not exist (default value), WebDAV basic authentication is disabled.

3.2.2.25 Disable basic authentication over a clear channel (SP 2 only)

HTTP basic authentication transmits the user name and password over the network in clear text. The only way to properly secure basic authentication would be to use a secure channel (SSL, or HTTPS). With this setting enabled, basic authentication will only succeed if the client and server are communicating over a secure channel.

By default, basic authentication is allowed over a clear channel. Setting this value to 1 requires the client and server to exchange basic authentication information over an encrypted channel.

Enabling this setting may prevent access to some web sites.

3.2.2.26 USB Block Storage Device Policy (SP2 only)

Most USB storage devices can be connected to a Windows workstation to provide extra storage capacity, or to move files between work and home. However, corporate policy may forbid moving sensitive files off of network storage and onto a removable device. The "Storage Device Policy" helps control use of these devices.

When enabled, the USB Block Storage Device Policy causes any USB mass storage devices to be mounted read-only, and files can not be saved to the device.

NOTE: At the time of this writing, this functionality was very limited, and applies only to devices using the standard Microsoft USB driver. Custom USB drivers are not affected by this policy.

3.2.2.27 DTC Access (SP2 only)

The Distributed Access Coordinator (DTC) service allows transactions to be coordinated and processed by multiple resources. The transactions may be all handled locally, or may be distributed across multiple machines.

With Service Pack 2, Windows now blocks all external DTC operations by default. However, additional registry settings are available should DTC transactions be required by an individual workstation. For more information on these registry settings, see Part 7 of the Changes to Functionality in Microsoft Windows XP Service Pack 2 document from Microsoft at http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/sp2otech.mspx.

4 Additional Security Protection

Many of the previous security related settings fell neatly into categories that were well defined, easy to implement, and easy to find. Beyond that, there are other requirements that do not fit into every mold – these are the things that make every computer unique. These may present the greatest challenge to securing a computer because these are more open-ended in nature. For lack of a better description, the pages that follow describe the realm that would fall into the category "*other*".

4.1 Available Services

Every piece of code that executes on a computer exists in a process. Many of these processes begin as "Services". You can view a list of processes by right-clicking "My Computer", and click "Manage". Expand "Services and Applications" and click "Services". These services are scheduled to start either at boot time, as normal Automatic or Manual startup, or disabled to not start at all.

The services listed below should be disabled to protect your computer against certain vulnerabilities. These services may also restrict certain functionality that you are accustomed to, but we have tried to maintain a reasonable level of functionality where possible.

Permissions on services listed here: **Administrators: Full Control; System: Read, Start, Stop, and Pause.** Permissions on services should be set using the Security template that accompanies the CIS Windows Scoring Tool.

4.1.1 Alerter

The alerter service is normally used to send messages between processes on one computer "alerting" the status of certain functions to the user's console, including the execution of print jobs. It also works in conjunction with the Messenger service to send these same messages between computers on a network.

The Alerter service is disabled by default with Windows XP Service Pack 2.

4.1.2 Automatic Updates

The Automatic Updates service was first published with Windows XP. It regularly checks the Microsoft web site in the background, and initiates the download of any new Critical Updates as they become available. It is designed to NOT use excessive network bandwidth. This service does not install anything itself, it makes updates ready to install.

NOTE: The Automatic Updates service and the Background Intelligent Transfer Service work together to help keep computers up to date with the latest critical patches. Organizations which have a separate patch management strategy should disable these services to prevent unmanaged system patching. Other organizations or individual users that do not have another method of patching should leave these services enabled and make use of this gift from Microsoft to keep patches up to date.

4.1.3 Background Intelligent Transfer Service (a.k.a. BITS)

The BITS service works in conjunction with the Automatic Updates service to download Critical Updates from Microsoft's Internet site, and make them available for installation. The service runs in the background, and makes use of unused and available bandwidth.

4.1.4 Clipbook

The Clipbook service is used to share clipboard information between computers on a network. In most cases, users don't want to share that information with other computers.

4.1.5 Computer Browser

The Computer Browser (not to be confused with Internet browsers, such as Internet Explorer or Netscape) keeps track of the computers on a network within a domain. It allows users to "browse" through Network Neighborhood to find the shared resources they need without knowing the exact name of that resource.

Unfortunately, it allows anyone to browse to those resources before checking any sort of authentication or authorization.

Disabling this service will require users to know the resources they are looking for, by name, and may result in an increased number of help desk calls.

4.1.6 Fax Service

The fax service is used for the unattended reception of incoming faxes. It is not required for the sending, or manual reception of faxes. It does require that a computer be left running all the time, and have the modem set to auto-answer.

Generally speaking, with the low cost of dedicated fax machines, the secure answer to most faxing needs would be to have a dedicated fax machine to receive faxes, while still using the computer to manually send faxes when appropriate.

4.1.7 FTP Publishing Service

The FTP Publishing Service is part of the Internet Information Server suite of Internet applications. It is not installed by default. It is used for making files on your local machine available to other users on your network or the Internet.

Generally speaking, workstations do not share files with other computers. This service should be disabled, or removed. If it is going to be installed, it should be properly maintained, which is a subject beyond the scope of this benchmark.

4.1.8 IIS Admin Service

Also part of the IIS suite of services, the IIS Admin Service manages the other IIS services. If this service is not running, the other services that are part of the IIS suite will not function either. Disable this service. If possible, this should be removed from workstations.

4.1.9 Indexing Service

This service indexes files on the system in an attempt to improve search performance. However, the service may occasionally consume excessive resources when compared to its usefulness.

4.1.10 Messenger

The Messenger service works in tandem with the Alerter service. It allows Alerter services of multiple computers to send alerts to each other over a network. Most users can live without the messenger and alerter services and still accomplish the tasks they need to do in the course of a normal day.

On October 15, 2003, Microsoft released Security Bulletin 03-043. This bulletin is an advisory of a vulnerability in the Messenger service that allows an attacker to execute application code of his or her choice. Disable this service to prevent this, or as-yet unknown similar vulnerabilities from affecting a system.

4.1.11 Net Logon

The Net Logon service establishes the NetLogon secure channel with a domain controller. See 3.2.1.18 above.

4.1.12 NetMeeting Remote Desktop Sharing

Microsoft has made one of the better collaboration tools that is available on the market today, but at the same time they took that tool – NetMeeting – and tried to make it into a remote control utility for help desk personnel to take control of your computer in time of need. In a world of hacker attacks and buffer overflows, it seems like only a matter of time before an exploit is discovered, or it is just abused. If you don't have a dedicated help desk, or your help desk doesn't use NetMeeting Remote Desktop Sharing, disable this service. If your organization requires this service, it should understand that there may be a risk involved.

4.1.13 Remote Desktop Help Session Manager

This service supports the Remote Assistance functionality. Disable the service to prohibit the use of Remote Assistance.

4.1.14 Remote Registry Service

The Windows Registry is essentially a database of settings and configuration options that affect almost every function of a Windows XP computer. It determines how everything behaves at startup, shutdown, and everything in between. The purpose of the Remote Registry Services is to expose that database to the rest of the network through a NetBIOS connection.

As frightening as that sounds, this service is enabled by default on every Windows computer deployed since the advent of Windows 95. A majority of remote administration tools have been written to take advantage of the Remote Registry Service to perform functions that would normally require a portion of their application to be installed locally.

Because of its widespread distribution, and its initial purpose, and the fact that it is still only protected by a username and password, the Remote Registry Service is responsible for opening the doors to uninvited guests as well as the remote management utilities it is used to support. Disable this service to prevent remote access to the system registry.

WARNING: By disabling this service, you are cutting any ability for support personnel or domain administrators to remotely manage your computer unless there is another application already installed on your computer to allow those functions. Be wary that this can break a large number of enterprise-wide applications.

4.1.15 Routing and Remote Access

The Routing and Remote Access service is normally used either to facilitate servers are Remote Access Servers, or to allow computers from one network to interact with computers on another.

RRAS is not fully implemented on Windows XP Professional like it is in the server operating systems. Users generally don't need RRAS on workstations. If this service can not be disabled, it should be locked down as much as possible. More information is available at http://www.microsoft.com/TechNet/columns/cableguy/cg0601.asp.

4.1.16 Simple Mail Transfer Protocol (SMTP)

Workstations are not normally used as SMTP mail servers. This service is installed as part of the IIS suite of applications. It should be disabled or removed entirely.

4.1.17 Simple Network Management Protocol (SNMP) Service

The Simple Network Management Protocol (SNMP) has long been the accepted standard for remote management through all network devices – routers, hubs, Unix, and Windows alike. It was recently discovered that SNMP has been proliferating a dangerously exploitable flaw for the past ten years or so. If you do not have a system actively using SNMP for remote management, disable it or remove it from the system.

4.1.18 Simple Network Management Protocol (SNMP) Trap

Another part of the SNMP protocol is the SNMP Trap service. Just like its counterpart, it should be disabled and/or removed.

4.1.19 Task Scheduler

The Task Scheduler service supports queuing batch programs for future execution. This could include virus scans, backups, or other system maintenance functions. With Windows XP, the task can run under alternate credentials, and does not necessarily have to run under the local system account.

4.1.20 Telnet

The Telnet service is not often installed on workstations. It is used for remote management of network devices, and offers a command-shell based form of network access to a computer. This is all well and good, but the traffic transferred by Telnet is not protected or encrypted in any way. If this is a requirement, take the time to look into a Secure Shell (SSH) remote management solution to fulfill your needs in a more secure manner. It is well worth the time and expense.

4.1.21 Terminal Services

Terminal services allow a remote graphical interface to the workstation. Similar to pcAnywhere or Virtual Network Client (VNC) software packages, Terminal Services share using the Remote Desktop Protocol (RDP). Normal use of the terminal service on a workstation terminates the existing interactive logon session; however, if remote assistance is enabled, any existing session can be shared between two computers.

4.1.22 Universal Plug and Play Device Host

Universal Plug and Play (UPnP) devices can be added to the network, and broadcast their availability for management. UPnP should not be confused with the more common Plug and Play (PnP) features useful for hardware management. UPnP finds devices on the network; PnP finds devices physically installed into the computer. Few devices on the market currently require UPnP, and this service should be disabled unless explicitly required.

4.1.23 World Wide Web Publishing Services

The grand-daddy of all exploitable services is Microsoft's World Wide Web service. It is the most often attacked web-server platform on the Internet today. As a result, it has had the most bugs found, and the most flaws exploited. This server is not installed by default, but should not exist on your average workstation. If it is not going to be properly maintained by personnel with an education in IIS security, it should be disabled or removed.

4.2 User Rights

In conjunction with many of the privileged groups in Windows XP, there are a number of individual rights that can be assigned to users or groups to grant them abilities that would be beyond the reach of normal users. Not all of these rights apply to Windows XP Professional, but many do.

4.2.1 Access this computer from the network

The ability to access a computer from the network is a user right that can be granted or revoked on any machine as appropriate. If this list is left empty, no user accounts can be used to gain access to the resources of this computer from the network.

4.2.2 Act as part of the operating system

The operating system works in a special security context called "LocalSystem". This security context has the ability to do things that normal users and administrative users can not. Granting this user right to users or groups will give them the ability to exceed normal privilege, regardless of their group membership.

4.2.3 Add workstations to domain

This user right only applies to domain controllers, and has no effect on Windows XP Professional.

4.2.4 Adjust memory quotas for a process

This policy setting defines the accounts which can adjust the maximum amount of memory assigned to a process.

4.2.5 Allow logon through terminal services

If terminal services are enabled, use this setting to explicitly control which users are allowed to remotely access the workstation.

4.2.6 Back up files and directories

This user right grants a user or group the ability to circumvent normal Windows file security for the purposes of backing up files and folders. It should be restricted when possible.

4.2.7 Bypass traverse checking

The Bypassing Traverse Checking user right allows access to files or folders regardless of the user's permissions to the parent folder. In other words, prevents the inheritance of permissions. Unfortunately, it is necessary to grant this right to users to allow normal operation of applications on a workstation.

4.2.8 Change the system time

Changing the system time on Windows XP computers is especially important to restrict in a domain environment because of the role that time synchronization plays in Kerberos authentication. This should not be configurable to anyone except Administrators.

4.2.9 Create a pagefile

In order to protect the potentially sensitive information that can be stored in a pagefile, the creation of pagefiles should be restricted to Administrators.

4.2.10 Create a token object

Allows the creation of a security access token. This right should never be given to any user.

4.2.11 Create permanent shared objects

The right to create permanent shared objects should only be used by applications in the Windows kernel. The kernel already has the right to create such objects, so no users should ever be granted this right.

4.2.12 Debug Programs

Any user can debug his or her programs, but this right allows a user to debug other processes on a machine. Users should not be granted this right except in an isolated development environment where possible.

Microsoft is soon to release new hot patching application technology that will require this right to apply patches. It promises fewer reboots for patches that need to be applied. In this light, Administrators still need this right to do their jobs. Hopefully, this will not be a permanent requirement, and can be eliminated in the future.

4.2.13 Deny access to this computer from the network

The “Deny Access” user rights always supercede the “Allow Access” user rights, so that if a user is listed under both user rights, that user will be denied access. If there are no users who should be allowed access to a computer from the network, the Everyone group should be listed in the “Deny Access to this computer from the network” user right.

4.2.14 Deny logon as a batch job

Just like the other “Deny…” user rights, a user listed here will be denied access to logon as a batch job, even if he has been explicitly granted that right.

4.2.15 Deny logon as a service

Just like the other “Deny…” user rights, a user listed here will be denied access to logon as a service, even if he has been explicitly granted that right.

4.2.16 Deny logon locally

Just like the other “Deny…” user rights, a user listed here will be denied access to logon to the console, even if he has been explicitly granted that right.

4.2.17 Deny logon through Terminal Service

Similar to the other “Deny…” rights, groups and accounts in this list will not be able to connect to the workstation using terminal services.

4.2.18 Enable computer and user accounts to be trusted for delegation

This user right only applies to Domain Controllers. It has no effect on Windows XP Professional.

4.2.19 Force shutdown from a remote system

This grants a user the right to shut down a computer from the network. It should only be granted to Administrators, and may be restricted to no users or groups at all.

4.2.20 Generate security audits

This user right allows a user or process to generate events to be added to the Windows Security Event Log.

4.2.21 Increase scheduling priority

The scheduling priority is one of the settings that can be altered as needed for performance tuning, but normal users should not have the ability to change the priority of other processes.

4.2.22 Load and unload device drivers

Device drivers execute as highly privileged applications on a Windows computer because they directly interface the hardware with the operating system. These drivers can be the source of “Trojan Horse” applications, and should be restricted where possible. This setting actually applies to the installation of Plug and Play device drivers.

4.2.23 Lock pages in memory

The right to lock pages in memory is the ability to force data in physical memory to remain in physical memory, and not be paged to disk, which can seriously degrade system performance. This user right is obsolete, and should remain empty.

4.2.24 Log on as a batch job

The right to log on as a batch job means that the listed user has the ability to log on using the batch queue facility. By default, Administrators have this right, but very rarely use it. Remove all users and groups from this right.

4.2.25 Log on as a service

Most applications that do not directly interact with the logged on user (and many that do) actually operate as a service. These services almost always execute under the LocalSystem security credentials. If a service needs to be executed in a user context, that user would have to be listed here.

4.2.26 Log on locally

Anyone who logs on locally to a computer must be listed here, either by individual user names, or by the “users” group.

4.2.27 Manage auditing and security log

The ability to manage the security event log is the equivalent to the ability for an intruder to cover his tracks and destroy evidence of what has been done to a computer system. This user right should be highly restricted, possibly even to only a subset of system administrators.

4.2.28 Modify firmware environment values

Individual users have the ability to change their own environment variables, but only Administrators and accounts that hold this right can change the environment variables of other users on a system.

4.2.29 Perform volume maintenance tasks

The most common volume maintenance tasks are “defrag” and “chkdsk”. In addition to the potential performance impact, this right could also allow low-level access to files bypassing standard permission constraints.

4.2.30 Profile single process

This user right grants the ability for one user to monitor the performance of another user or non-system process.

4.2.31 Profile system performance

The Profile system performance user right allows a user or group of users to monitor system performance, including system processes.

4.2.32 Remove computer from docking station

This user right is just what you’d expect.

4.2.33 Replace a process level token

The ability to replace a process level token essentially means that a process can change the authentication authority of its own child-processes.

4.2.34 Restore files and directories

In conjunction with the “Backup files and directories” user right, this can be very dangerous if a user backs up certain security related information, alters it, and restores it back to the same place. It should be restricted to Administrators.

4.2.35 Shut down the system

Users granted this right have the ability to shut down the computer. This only takes effect if users are required to log on to shut down a system.

4.2.36 Synchronize directory service data

This user right has no effect on Windows XP Professional.

4.2.37 Take ownership of file or other objects

A user who “owns” a file has greater authority over that file than even the permissions would suggest. The right to take ownership of a file is equivalent to the ability to compromise an entire file system.

4.3 Other System Requirements

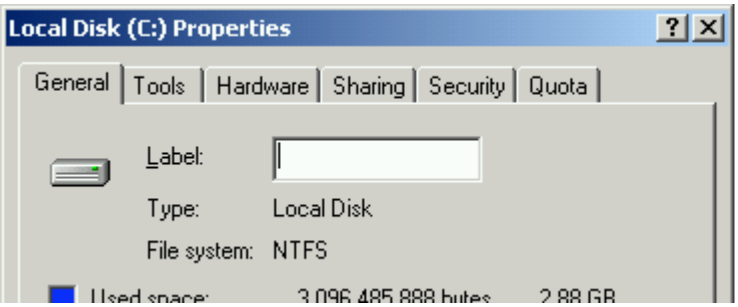
4.3.1 Ensure all disk volumes are using the **NTFS file system**

Warning: Do not do this if your system is a dual-boot system with Windows 95/98/Me. The alternate operating system will cease to function, and can not be recovered.

Since the early days of DOS, files have been stored on floppy disks. These disks break up data into blocks, and those blocks are written to similar blocks on a physical disk. The “map” describing which blocks are holding which files is stored on part of the disk called the “File Allocation Table” or FAT. When DOS moved to Hard Disks, the same FAT style of disk allocation was used. FAT filesystems had some good points – most of all, it’s pretty simple. Any system could read the disks, and if there was a problem, the data could have been restored. When disks began to grow beyond the size of FAT’s capabilities, it was expanded to FAT32, allowing for larger disks. However, FAT and FAT32 do not offer any security.

NTFS interoperability has come a long way since its initial introduction. It can be bypassed if the system can be rebooted, but it is the ONLY way that any file-level security can be enforced while system is operating.

To determine if a disk volume is NTFS, double click “My Computer” on the desktop. Right-click the C drive (C:) and click Properties. The properties pane for that disk will describe the “File System” as either FAT or NTFS.



Label:

Type: Local Disk

File system: NTFS

Used space: 3,096,485,888 bytes 2.88 GB

In order to make a FAT disk into an NTFS disk, open a Command Prompt (Click Start -> Programs -> Accessories -> Command Prompt) and type “Convert C: /fs:ntfs”. The system will probably be required to restart to perform this task. Take the same action with the D: drive and any others that show up as FAT disks.

Once the disks have been converted to the NTFS file system, default security must be applied to the boot drive (C:). Open a command prompt (click Start, Programs, Accessories, and Command Prompt) and type the following command for workstations:

“secedit /configure /db default.sdb /cfg %windir%\inf\defltwk.inf /areas filestore”

or the following command for servers:

“secedit /configure /db default.sdb /cfg %windir%\inf\defltsv.inf /areas filestore”

and press enter. The /db parameter is required, even though the database does not exist until after the command is run. Type “secedit /?” for more information on this command.

Other applications will have the ability to use these security features. Most users never need to update these file permissions, while system administrators of all levels will need to do so from time to time. In fact, it is possible to cripple a system by incorrectly modifying that security. It is important to keep in mind that this is still a step up from a FAT filesystem with NO security.

4.3.2 NetBIOS on all network devices

By default, the XP workstation will use both NetBIOS and DNS transports in attempting to locate shared resources such as files and printers. However, Windows 2000 introduced the ability to eliminate NetBIOS and WINS for locating resources, in favor of a direct TCP connection through DNS.

Disabling NetBIOS reduces the services running on the workstation. The NetBIOS name service runs on TCP and UDP port 137, the datagram service listens on UDP port 138 and the session service listens on TCP port 139. All SMB resource sharing applications will use TCP and UDP port 445, and ports 137, 138 and 139 can be firewalled.

NetBIOS can only effectively be disabled if all shared resources on the client network run on Windows 2000 or later.

See Microsoft Knowledge Base article 299977 for additional items to consider when disabling NetBIOS. Also see Knowledge Base article 315267 for information on how to disable NetBIOS on Windows XP.

Warning: Disabling NetBIOS is NOT supported by Microsoft and can result in loss of functionality and unstable/unpredictable system behavior. Proper testing should be conducted on **non-production** systems to determine the impact of disabling NetBIOS on your systems/networks.

4.3.3 Enable the Windows Firewall on all network devices.

In general, the Windows Firewall is available only when you are connected directly to the Internet, but not for Local Area Network (LAN) connections. The firewall is also enabled on dial-up internet connections and shared internet connections.

When enabled, the Windows Firewall blocks inbound traffic to your workstation unless a port is explicitly opened. The Windows Firewall typically is not necessary on internal networks where a firewall already exists between the client and the untrusted network. The Windows Firewall also supports activity logging.

For more information about the Windows Firewall on Windows XP, see Microsoft Knowledge Base Article 320855.

4.3.4 Restricted Groups

With Restricted Groups enabled, the operating system will evaluate local group membership on boot and when group policy refreshes. Members in the "Restricted Groups" policy are compared against the actual, current group membership. If the accounts listed in the policy are not in the group, they are added. Conversely, if an account is in the group but not in the policy, it is removed.

4.3.4.1 Remote Desktop Users

Use this policy to explicitly control which users are allowed to use the remote desktop service (Terminal Services).

4.4 File and Registry Permissions

Once a volume has been converted to NTFS, and once the basic file security settings have been applied, additional settings should be applied. Most known operating system and application exploits exist because of multiple factors. First, there is an application that has a flaw that opens a low-privileged door into an operating system. And second, that open door allows a knowledgeable intruder to elevate his privilege and take over the system. The permissions listed below will help to make an operating system "resistant" to privilege elevation, even to potential software vulnerabilities that have not yet been discovered.

WARNING: It is possible that the permissions applied here can take away some sort of application functionality that you are accustomed to. If that happens and you need to back off to a previously known state, use the same instructions that were used to apply the basic permissions to a freshly converted NTFS file system to "undo" most of the settings you see below.

4.4.1 File Permissions

* Unless stated otherwise, Administrators or System Full Control is full control for the designated folder and all contents. Creator Owner Full Control is for subfolders and files only. Users permissions are for current folder, subfolders, and files. Files listed with an "a.k.a." may be listed on "%SystemDrive%" or on "C:\", so both entries are included in the accompanying template.

4.4.1.1 %SystemRoot%\system32\at.exe – SYSTEM, Administrators
4.4.1.2 %SystemRoot%\system32\attrib.exe – SYSTEM, Administrators
4.4.1.3 %SystemRoot%\system32\cacls.exe – SYSTEM, Administrators
4.4.1.4 %SystemRoot%\system32\debug.exe – SYSTEM, Administrators
4.4.1.5 %SystemRoot%\system32\drwatson.exe – SYSTEM, Administrators
4.4.1.6 %SystemRoot%\system32\drwtsn32.exe – SYSTEM, Administrators
4.4.1.7 %SystemRoot%\system32\edlin.exe – SYSTEM, Administrators, INTERACTIVE
4.4.1.8 %SystemRoot%\system32\eventcreate.exe – SYSTEM, Administrators
4.4.1.9 %SystemRoot%\system32\eventtriggers.exe – SYSTEM, Administrators
4.4.1.10 %SystemRoot%\system32\ftp.exe – SYSTEM, Administrators, INTERACTIVE
4.4.1.11 %SystemRoot%\system32\net.exe – SYSTEM, Administrators, INTERACTIVE
4.4.1.12 %SystemRoot%\system32\net1.exe – SYSTEM, Administrators, INTERACTIVE
4.4.1.13 %SystemRoot%\system32\netsh.exe – SYSTEM, Administrators
4.4.1.14 %SystemRoot%\system32\rcp.exe – SYSTEM, Administrators
4.4.1.15 %SystemRoot%\system32\reg.exe – SYSTEM, Administrators

4.4.1.16 %SystemRoot%\regedit.exe – SYSTEM, Administrators
4.4.1.17 %SystemRoot%\system32\regedt32.exe – SYSTEM, Administrators
4.4.1.18 %SystemRoot%\system32\regsvr32.exe – SYSTEM, Administrators
4.4.1.19 %SystemRoot%\system32\rexec.exe – SYSTEM, Administrators
4.4.1.20 %SystemRoot%\system32\rsh.exe – SYSTEM, Administrators
4.4.1.21 %SystemRoot%\system32\runas.exe – SYSTEM, Administrators, INTERACTIVE
4.4.1.22 %SystemRoot%\system32\sc.exe – SYSTEM, Administrators
4.4.1.23 %SystemRoot%\system32\subst.exe – SYSTEM, Administrators
4.4.1.24 %SystemRoot%\system32\telnet.exe – SYSTEM, Administrators, INTERACTIVE
4.4.1.25 %SystemRoot%\system32\tftp.exe – SYSTEM, Administrators, INTERACTIVE
4.4.1.26 %SystemRoot%\system32\tlntsvr.exe – SYSTEM, Administrators

5 Administrative Templates

5.1 System

5.1.1 Remote Procedure Call

The Remote Procedure Call (RPC) security model has been enhanced for Windows XP service pack 2. RPC is used to publish services on non-standard TCP ports. A client locates services by connecting to the RPC endpoint mapper (which runs on a standard port) and querying the server for a specific service.

Service pack 2 allows the administrator to require authentication to connect to the endpoint mapper. Additionally, the administrator can specify global authentication requirements which must be met before connecting to any RPC service.

Important: The NetSchedule legacy interface uses RPC to communicate with the Scheduler service This interface is most commonly used by AT.EXE or other legacy scheduling applications, and does not support authentication. *AT.EXE will no longer work when RPC authentication is required through policy.*

5.1.1.1 RPC Enpoint Mapper Client Authentication (SP2 only)

By default in Service Pack 2, the RPC endpoint mapper can not be accessed by anonymous clients. It may be necessary to set this to “disabled” for RPC applications which do not support authentication.

5.1.1.2 Restrictions for Unauthenticated RPC clients (SP2 only)

By default in Service Pack 2, all RPC services require authentication in order to connect, and all anonymous calls are rejected. Authentication can be disabled through policy.

Some applications could be written to explicitly invoke RPC callbacks without authentication, and bypass these new restrictions (the RPC_IF_ALLOW_CALLBACKS_WITH_NO_AUTH flag). This is a new option, and does not apply to legacy applications. By default, applications registered this way will bypass authentication even when “Restrictions for Unauthenticated RPC clients” is enabled. However the administrator may choose to require even these services to be authenticated using the setting “Authenticated without exceptions.”

5.2 Network

5.2.1 Network Connections

5.2.1.1 Windows Firewall

Windows XP Service Pack 2 contains significant improvements to the Windows Firewall. The firewall supports remote management, and a wide array of configuration options through group policy.

The Windows Firewall blocks inbound traffic only. Except for ICMP traffic, no configuration or filter options are provided for controlling outbound packets.

IPv6 support is included in the Windows Firewall by default.

Note that the Windows Firewall may defeat the remote operation of many Microsoft Management Console (MMC) snap-ins, including Computer Management, Disk Management, Event Viewer, Resultant Set of Policy, Services, and many others. For more information, see Microsoft Knowledgebase Article 840634, http://support.microsoft.com/default.aspx?scid=kb;en-us;840634.

WARNING: Firewall settings, even more than most of the other security settings in this guide, must be tailored to your site. Testing is critical before deploying a firewall configuration for your site. Improper firewall settings could block critical applications such as anti-virus or desktop management agents. In some instances, improper firewall settings could even block Active Directory and group policy management of the machine, leaving no easy way to undo changes.

5.2.1.1.1 Domain Profile

The firewall supports two separate profiles. The domain profile applies only to computers which are joined to a domain, and has no effect on workgroup machines. When a domain computer is connected to the corporate network, typically a less strict policy can be applied.

5.2.1.1.1.1 Protect all network connections (SP2 only)

By default, all network interfaces are protected by the Windows Firewall service. If this setting is disabled, the setting specified in the administrative template Network\Network Connections\Prohibit use of Internet Connection Firewall" takes effect.

5.2.1.1.1.2 Do not allow exceptions (SP2 only)

The firewall policy gives the administrator fine-grained control over allowed and prohibited network traffic. However, when "Do not allow exceptions" is enabled, the firewall blocks all traffic, and ignores exceptions defined below.

5.2.1.1.1.3 Allow local program exceptions

When a program is defined as an exception, it can receive unsolicited network traffic on any port it requests the firewall to open. Windows supports two program exception lists: one defined in group policy, and another defined locally through the machine's control panel.

Enabling this setting allows the system administrator to specify programs which may receive incoming network traffic, and bypass Windows Firewall restrictions.

5.2.1.1.1.4 Allow remote administration exception

In a corporate environment, various systems may be used to query and manage workstations. These systems might remotely connect to the registry to read patch information, connect to the file system to retrieve logs, or use Windows Management Instrumentation (WMI) to read various system parameters.

When remote administration is enabled, the Windows Firewall service opens TCP ports 135 and 445. It also allows SVCHOST.EXE and LSASS.EXE to receive incoming traffic on dynamic ports.

This setting can be opened to all hosts, to the local subnet, or to a specific IP address range.

5.2.1.1.1.5 Allow file and printer sharing exception (SP2 only)

In order for a workstation to share files or locally connected printers, this setting must be enabled. This does not need to be enabled for the client to connect to files on another machine, or to access a remote printer.

When enabled, this setting allows inbound traffic on UDP ports 137 and 138, and TCP ports 139 and 445.

5.2.1.1.1.6 Allow ICMP exceptions (SP2 only)

Internet Control Message Protocol (ICMP) traffic is used to respond to non-transient network problems. ICMP traffic differs from TCP and UDP traffic, and is used primarily to manage the network itself, and not to send application data. However, malicious applications have been known to use ICMP traffic as a data channel.

The windows firewall provides granular control over exactly which ICMP messages are accepted and sent. For more information on specific ICMP messages, refer to RFC 792, “Internet Control Message Protocol.”

5.2.1.1.1.7 Allow Remote Desktop exception (SP2 only)

The remote desktop protocol gives a remote administrator full access to the workstation’s graphical interface. It can be through a separate session, or they can share the session with a logged on user. This feature is often useful for troubleshooting, and is used by the Remote Assistance service.

When Remote Desktop is allowed, the Windows Firewall allows inbound connections on port 3389. Like other network settings, this can be granted all users, to the local subnet, or to a specific IP subnet.

5.2.1.1.1.8 Allow UPnP framework exception (SP2 only)

When Universal Plug-n-Play (UPnP) is enabled, the computer can receive unsolicited PnP messages. By enabling this policy, you open TCP port 2869 and UDP port 1900 on the Windows firewall.

5.2.1.1.1.9 Prohibit notifications

Typically, when an application attempts to open up a network port to listen for unsolicited traffic, the user is notified, and given the option of whether or not to allow this behavior. If this option is disabled through policy, the display is prohibited and the connection is blocked.

If this policy is not configured, an administrator can access the Windows Firewall through the control panel and enable this notification.

5.2.1.1.1.10 Allow logging (SP2 only)

When logging is enabled, the Windows firewall writes information about network connection to a log file. The size of the file is controlled by policy. You have the option of logging all connection information, or just information about dropped connections.

5.2.1.1.1.11 Prohibit unicast response to multicast or broadcast (SP2 only)

Often traffic can be sent to a broadcast address. Hosts may choose to respond to broadcast traffic; if so, a single incoming broadcast packet can generate a large number of unicast reply packets to the sender. This can result in a denial-of-service attack.

Configure this setting to disable responses to multicast or broadcast packets.

If muticast networking is supported in your environment, this setting should be enabled.

5.2.1.1.1.12 Define port exceptions (SP2 only)

You may choose to open specific ports for your entire domain environment. For example, your anti-virus or patch management agents may listen for incoming connections on a specific port. If so, you can configure all clients to leave this port open through group policy by defining it as a port exception.

5.2.1.1.1.13 Allow local port exceptions (SP2 only)

Port exceptions can also be made on a per-machine basis. If this setting is enabled, an administrator can open specific ports (e.g., HTTP on port 80) for individual specific machines through the Windows Firewall settings in the control panel.

5.2.1.2 Standard Profile

The Windows Firewall also uses a "Standard" profile, which offers the same settings as the Domain profile. However, the standard profile is applied to domain workstations when a domain controller is not available. This becomes particularly useful for corporate laptops, and allows the administrator to enforce a stricter security policy when the device is connected to a non-secured network.

Computers that are members of a workgroup (i.e., not joined to a domain) always use the Standard profile.

Warning: The "Standard Profile" firewall settings defined in this guide assumes that the computer belongs to a domain. **These settings are probably not appropriate for a small office, home office or workgroup machine. They also may not be appropriate for large corporations with machines that regularly move between domains**. Rather, they are designed to protect a device such as a mobile laptop that moves off the trusted corporate network and onto an untrusted public network. The standard profile outlined in this policy will protect the computer when it is on the untrusted network.

5.3 Windows Components

5.3.1 Security Center

5.3.1.1 Turn on Security Center (Domain PCs only) (SP2 only)

The Security Center is useful for displaying significant alerts to the user. By default, the security center is enabled, and will alter the user when the computer has a degraded security posture. The Security Center monitors three critical items:

- Anti-virus software is running, and signatures are up-to-date. This feature can be disabled by setting the registry key HKLM\SOFTWARE\Microsoft\Security Center\AntiVirusDisableNotify to 1.
- The windows firewall is running. This feature can be disabled by setting the registry key HKLM\SOFTWARE\Microsoft\Security Center\FirewallDisableNotify to 1.
- The Windows Update Service is running, and all current updates have been applied. This feature can be disabled by setting the registry key HKLM\SOFTWARE\Microsoft\Security Center\UpdatesDisableNotify to 1.

Appendix A: Windows Security Questionnaire

The Windows XP Professional Security Benchmarks represent a general consensus of steps that can be taken to allow most of the normal functionality of a Windows XP Professional computer, while mitigating many common Internet risks. These settings have been presented in Section 1, and then described in greater detail in Section 2. These two sections together constitute the CIS Windows XP Professional Security Benchmark.

In addition to the configurations described above, there is a great deal more that can be done, depending on what role your computer fulfills, and what type of computer environment you are in. Well managed environments that have full time computer security support professionals may not have a great deal of need for this appendix, but there are a great many businesses, with or without dedicated personnel, who may be able to protect themselves better with help from this question-and-answer session.

1. **Does anyone on another computer use shared files or printers from your computer?**

   Yes: Your Windows XP Professional computer is already capable of sharing files and printers with other computers on your network.

   Do This: Go on to the next question.

   No: In addition to the steps already taken, you can DISABLE file and printer sharing and deny remote access to your computer entirely!

   Do This: Disable File and Printer Sharing:
   - Click Start -> Settings -> Network and Dial-Up Connections.
   - Right-click each active connection, and click Properties.
   - Un-check the box for "File and Printer Sharing for Microsoft Networks".
   - Click OK.

   Do This: Deny all access from Network users:
   - Click Start -> Settings -> Control Panel.
   - Double-click Administrative Tools.
   - Double-click Local Security Policy.
   - Navigate to Local Policies -> User Rights Assignment.
   - Double-click "Deny Access to this computer from the network".
   - Click Add.
   - Double-click "Everyone" and click OK.
   - Click OK again, and close all open windows.

2. **Does your computer use resources (files or printers) stored on any other computers on your network, other than Internet mail or Internet Browsing?**

   Yes: Your Windows XP Professional computer is already capable of sharing files and printers with other computers on your network.

   No: In addition to the steps already taken, you can DISABLE all Microsoft networking and deny remote access to your computer entirely!

Do This: Disable Microsoft Networking

- Click Start -> Settings -> Network and Dial-Up Connections.
- Right-click each active connection, and click Properties.
- Un-check the box for “Client for Microsoft Networks”.
- Click OK.

Appendix B: Internet Resources

The Center for Internet Security – http://www.cisecurity.org

The SANS Institute – http://www.sans.org

National Security Agency Security Recommendation Guides – http://www.nsa.gov/ia

Department of Defense recommendations – not currently available online.

Microsoft Windows Security – http://www.microsoft.com/security
Windows XP Security Guide – http://go.microsoft.com/fwlink/?LinkId=14839
Server 2003 Security Guide – http://go.microsoft.com/fwlink/?LinkId=14845
Threats and Countermeasures Guide – http://go.microsoft.com/fwlink/?LinkId=15159

Microsoft Directory Services Client for Windows 9x/Me -
http://www.microsoft.com/TechNet/prodtechnol/ntwrkstn/downloads/utils/dsclient.asp?frame=true

Windows NT Magazine article regarding editing the Registry -
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winntas/tips/winntmag/inreg.asp

NIST Windows 2000 Security Guidelines - http://csrc.nist.gov/itsec/guidance_W2Kpro.html

Appendix C: Problematic Settings

In the course of developing any type of security standard, there is one perpetual constant: Something will be broken. When you change something in favor of increasing security, you are "breaking" a potentially vulnerable or exploitable program.

An unfortunate side-effect of disabling the unwanted services is the likelihood that some hazardous program or function has also been used for good instead of evil. The unfortunate part is that when you disable the risky code, a perfectly viable operation is also disabled.

In an effort to disclose likely sources of problems, this appendix lists some of the settings that are known to cause problems, and what types of problems may arise. This is not an all-inclusive list. It is provided in good faith to help you diagnose problems when securing systems. It is subject to change as information becomes available.

3.1.1: Additional Restrictions for Anonymous connections "No Access Without Explicit Anonymous Permissions". Many older applications (and some new ones) actually use Null Sessions to communicate between computers, or between processes on the same computer. If an application fails to work once a computer is "locked down" this should be the first setting to "undo" while troubleshooting.

3.2.1.47: Lan Manager Authentication Level set to "Send NTLMv2 response only". This setting will make a Windows XP computer unable to share resources with other computers that are not set to use NTLMv2. It will make the computer unable to share resources with Windows 95/98/Me computers unless they install the DSCLIENT.EXE application from the Windows 2000 installation CD.

3.2.1.12: Restrict CD-ROM Access to Locally Logged-On User Only. One problem has been identified when this setting is enabled. When users are installing software from a CD-ROM drive, and those installation packages use the Microsoft Installer (.MSI) packages, the software is actually installed by the Windows Installer service, NOT the local user. If this setting is enabled, such software installation will not be able to proceed, because of this restriction. The setting must be changed long enough to install the software, or the package must be copied to a local or network drive for the installation procedure to succeed.

3.2.2.9: Remove administrative shares on workstation (Professional): **HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters\AutoShareWks (REG_DWORD) 0.** Removing administrative shares on Windows computers is entirely desirable if they are not going to be used. This is likely to break some applications that use administrative shares – the most notable of which are backup and restore utilities.

4.4: File and Registry Permissions. It should go without saying that if a user or application is attempting to access an object, and receiving an "Access Denied" error, that some attention should be paid to the permissions applied to that object.

Appendix D: Windows XP Service Pack 2

Windows XP introduced a number of significant security enhancements. Most of the significant security enhancements break down into these ten general categories:

1. Bluetooth.

Windows XP now provides out-of-the-box support for Bluetooth connections. Bluetooth is most commonly used for short distance communications, and makes its mark as a replacement for infrared connections. Although Bluetooth operates in the same frequency range as 802.11 wireless networks, it serves a very different purpose. Once Bluetooth is configured for use on a workstation, you can access configuration options through the control panel.

Some examples of Bluetooth connections include the following:

- Dial-up networking to connect your PC to a Bluetooth-enabled mobile phone
- Printing to a Bluetooth-enabled printer
- Host interface wireless devices such a mouse or keyboard.
- Personal networking which creates an IP connection between two Bluetooth enabled devices

Bluetooth obviously presents some security concerns. However, at this time, there are no native configuration options to manage these connections. Therefore, this guide does not currently include provide any Bluetooth recommendations.

2. DCOM Permissions.

Windows machines typically host a number of DCOM services. These services can be accessed locally by the workstation itself, or remotely from another machine. Although local and remote calls are handled somewhat differently, they both end up passing through the same COM engine.

Service Pack 2 adds group policy settings which control permissions for managing DCOM components. Permissions are separated into two distinct categories: users that can access existing DCOM services, and users that can launch or activate services. Rights are typically assigned depending on whether the DCOM request came from the machine itself (local), or from another machine (remote).

These settings are discussed in sections 3.2.1.9 and 3.2.1.10.

3. RPC Permissions.

RPC services behave similar to DCOM services. They allow a remote computer to access a service on the workstation. Each separate service requires a TCP port to be opened on the workstation. Rather than assigning specific ports to each service, the operating system provides a generic “portmapper.” The portmapper serves as an address book, allowing clients to determine which port is assigned to a specific DCOM service.

With Service Pack 2, Microsoft by default requires all clients to authenticate before being allowed to connect to a service on the workstation. In addition, clients must authenticate before being allowed to query the portmapper to locate a specific DCOM service.

Section 5.1.1 describes administrative template settings used to control DCOM access permissions.

4. WebDAV Permissions.

Web (HTTP) based file management is becoming increasingly popular. Using the standard HTTP protocol, clients can access, modify and delete files on a remote server. As the protocol developed, Microsoft embedded the technology more deeply into the operating system. Within XP, you are able to access files using WebDAV through the same interface used to access network shares with NetBIOS or SMB.

The HTTP protocol uses different authentication methods from traditional Windows networking protocols. Many systems support some robust authentication models through HTTP, such as Kerberos or NTLM. However, clients and servers can also negotiate "Basic" HTTP authentication, which essentially passes credentials across the network in clear text.

Service pack 2 introduced two new settings to protect credentials sent over HTTP sessions. These settings are discussed in sections 3.2.2.24 and 3.2.2.25.

5. Windows Firewall.

The most significant security improvement with Windows XP Service Pack 2 is the Windows Firewall. By default, the firewall service is enabled, and monitoring inbound traffic on all interfaces. The service provides many very specific settings for controlling published network ports. In addition, the service works in combination with the RPC interface to effectively control remote access to specific RPC services, which may be dynamically assigned listening ports.

All settings for the firewall can be managed through group policy, as described in 5.1.2.2.1.

6. Wireless Provisioning Services.

The WiFi industry has been working rapidly to recover from significant security vulnerabilities identified in the initial implementation of 802.11 wireless networks. Service Pack 2 provides access to the improved security options through a new feature called "Wireless Provisioning Services."

Wireless provisioning services provide additional controls for three specific scenarios: the public Hotspot provider, a generic wireless Internet Service Provider, and the corporate network. By using a Wireless Network Registration Wizard and Setup Wizard, the client can safely connect to a service provider on an encrypted channel without having to exchange cumbersome passwords.

At this point, no native configuration options exist to control these new wireless configuration settings. Therefore, this guide does not provide any recommended settings for Wireless Provisioning Services.

7. Data Execution Protection.

The most significant class of vulnerabilities remains the Buffer Overflow. With a properly crafted exploit, an attacker can easily shut down specific services, an sometimes even gain full control over a computer. The root problem seems extremely simple: the attacker stuffed too much data into memory. The extra data flowed over into an area of memory designated for something else—such as executable code—and compromised the machine.

Windows XP Service Pack 2 provides additional protection against buffer overflows in two ways. First, the operating system can work with the hardware to identify specific parts of memory as “Non Executable”—NX regions. However, this requires hardware which supports such protection. Alternatively, the operating system can perform similar protection in code. *It is not necessary to upgrade to new hardware to benefit from Windows Data Execution Protection.*

Since buffer overflows have played such a significant role in past security vulnerabilities, this protection is considered critical in protecting the machine. Data Execution Protection is discussed in section 3.1.3.

8. The Security Center.

The Security Center continually monitors the three cornerstones of security on the workstation: anti-virus software, the firewall and the security updates service. When an issue arises with any of these three items, the security center notifies the user. Individual items can be disabled through registry keys.

The security center is discussed in section 5.3.

9. DTC Control.

Transactions can be coordinated across multiple processes using the Distributed Transaction Coordinator (DTC). The process could all be local to a single machine, or they could be spread across a number of devices—file systems, message queues and databases, for example.

Workstations rarely need to be involved in network-based distributed transactions. In order to reduce the attack surface of the workstation, this service has been disabled by default. The registry setting used to manage DTC settings is discussed in section 3.2.2.27.

10. Outbound Connection Throttling

Service Pack 2 limits the number of incomplete outbound TCP connection attempts. If an application (such as a port scanner) generates a large number of outbound connection requests, the requests are throttled, since this activity is not normal. When throttling occurs, event 4226, source “Tcpip” is written to the system event log.

Appendix E: Change History

November 6, 2003 – Version 1.0 released to public.

March 13, 2004 – Version 1.1.2 released.
Updated changes to "Debug Programs" User Right.

September 3, 2004 – Version 1.2 released.
Added section on "Security Levels"
Updated "High Security" template to comment out the SystemDrive, HKLM\Software, and HKLM\System permissions. Administrators must manually edit the template to enable these settings.

October 3, 2004 – Version 1.2.1 released.
Fixed references in Appendix C.
Resolved typographical errors in HiSec Template.

October 20, 2004 – Version 1.3 released.
Renamed "High Security" to "Specialized Security – Limited Functionality".

August 22, 2005 – Version 2.0 released.

- Renumbering to accommodate added SP2 items.
- Item 2.2.4.1.2: Changed to "As Needed"
- Item 2.2.4.2.3: Changed to "As Needed"
- Item 2.2.4.3.3: Changed to "As Needed"
- Item 3.1.4 added.
- Item 3.2.1.6: Specialized level changed to "Disabled"
- Item 3.2.1.7: Specialized level changed to "Disabled"
- Item 3.2.1.8: Specialized level changed to "Not Defined"
- Item 3.2.1.9: added; previous item moved to 3.2.1.11
- Item 3.2.1.10: added; previous item moved to 3.2.1.12
- Item 3.2.1.13: Enterprise settings changed to "Enabled" and "Not Defined"
- Item 3.2.1.14: Specialized level changed to "Disabled"
- Item 3.2.1.15: Specialized level changed to "Disabled"
- Item 3.2.1.44: Added list of registry paths to Specialized level
- Item 3.2.1.45: Legacy and Enterprise levels change to "Not Defined". Specialized level changed to "COMCFG, DFS$"
- Item 3.2.1.50: "Require" changed to "Negotiate"
- Item 3.2.1.53: Specialized level changed to "Disabled"
- Item 3.2.1.56: Specialized level changed to "Disabled"
- Item 3.2.1.57: Enterprise and Specialized levels changed to "Not Defined"
- Item 3.2.1.58: Changed to "CREATOR OWNER"
- Item 3.2.2.1: Legacy and Enterprise changed to "Not Defined"
- Item 3.2.2.2: Changed to "Not Defined"
- Item 3.2.2.6: Changed to "Not Defined"
- Item 3.2.2.7: Legacy and Enterprise changed to "Not Defined"
- Item 3.2.2.10: Changed to "Not Defined"
- Item 3.2.2.12: Legacy and Enterprise changed to "Not Defined"
- Item 3.2.2.13: Legacy and Enterprise changed to "Not Defined"

- Item 3.2.2.14: Changed to “Not Defined”
- Item 3.2.2.15: Legacy and Enterprise changed to “Not Defined”
- Item 3.2.2.16: Legacy and Enterprise changed to “Not Defined”
- Item 3.2.2.17: Legacy and Enterprise changed to “Not Defined”
- Item 3.2.2.18: Legacy and Enterprise changed to “Not Defined”
- Item 3.2.2.19: Changed to “Not Defined”
- Item 3.2.2.20: Changed to “Not Defined”
- Item 3.2.2.22: Legacy and Enterprise changed to “Not Defined”
- Item 3.2.2.25: Legacy and Enterprise changed to “Not Defined”
- Item 3.2.2.26: Legacy and Enterprise changed to “Not Defined”
- Item 3.2.2.27: Legacy and Enterprise changed to “Not Defined”
- Item 4.1.11: Changed to “Not Defined”
- Item 4.1.14: Changed to “Not Defined”
- Item 4.2.1: Changed to “Not Defined”
- Item 4.2.5: Legacy and Enterprise changed to “Not Defined”
- Item 4.2.6: Changed to “Not Defined”
- Item 4.2.7: Changed to “Not Defined”
- Item 4.2.12: Legacy changed to “Administrators”
- Item 4.2.13: Added “Support_388945a0”
- Item 4.3.2: Changed to “Not Defined”
- Added Section 5: Administrative Templates for SP2 items

August 30, 2005 – Version 2.01

- Removed Appendix C because it was out of date
- Typo and other text corrections.
- Item 3.2.1.56: Specialized level changed to Enabled.