NIST
National Institute of
Standards and Technology
Technology Administration
U.S. Department of Commerce

Special Publication 800-43

Systems Administration Guidance for Securing Microsoft Windows 2000 Professional System

Recommendations of the National Institute of Standards and Technology

Murugiah Souppaya
Anthony Harris
Mark McLarnon
Nikolaos Selimis

This page intentionally left blank

NIST Special Publication 800-43

Systems Administration Guidance for Securing Microsoft Windows 2000 Professional System

Recommendations of the National Institute of Standards and Technology

Send Comments to itsec@nist.gov

C O M P U T E R S E C U R I T Y

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

November 2002

U.S. Department of Commerce
Donald L. Evans, Secretary

Technology Administration
Phillip J. Bond, Under Secretary for Technology

National Institute of Standards and Technology
Arden L. Bement, Jr., Director

This page intentionally left blank

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This Special Publication 800-series reports on ITL's research, guidance, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Special Publication 800-43
Natl. Inst. Stand. Technol. Spec. Publ. 800-43, 192 pages (November 2002)
CODEN: XXXXX

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 2001

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov — Phone: (202) 512-1800 — Fax: (202) 512-2250
Mail: Stop SSOP, Washington, DC 20402-0001

Acknowledgements

The authors Murugiah Souppaya of NIST and Anthony Harris, Nikolaos Selimis, and Mark McLarnon of Booz Allen Hamilton wish to thank Timothy Grance and John Wack, staff at NIST, the National Security Agency, Steve Lipner, Jesper Johansson, and Kirk Soluk from Microsoft, and the entire Security Professional community for providing valuable contributions to the technical content of this guide. Additionally, the authors also thank the Defense Information Systems Agency (DISA), the Center for Internet Security (CIS), and SysAdmin Network Security Institute (SANS) for their valuable contributions to the baseline and their continued efforts to improve security in this and in other similar efforts.

Trademark Information

Table of Contents

Executive Summary **ES-1**

1. Introduction **1-1**

1.1 Authority 1-1
1.2 Purpose and Scope 1-1

2. Windows 2000 Security Components Overview **2-1**

2.1 Kerberos Support 2-1
2.2 Smart Card Logon Support 2-1
2.3 PKI Support 2-2
2.4 IPsec Support 2-2
2.5 PPTP And L2TP Support 2-3
2.6 Encrypting File System Support 2-3

3. Stand-Alone Versus Domain Member **3-1**

3.1 Stand-Alone 3-1
3.2 Domain 3-1

4. Security Configuration Tool Set **4-1**

4.1 Windows 2000 Security Templates 4-1
4.2 Analysis and Configuration 4-2
4.3 Group Policy Distribution 4-5
4.4 Secedit 4-6
4.4.1 Secedit Syntax 4-6
4.4.2 Secedit Advantages 4-6
4.5 Creating Security Templates 4-6
4.6 Summary of Recommendations 4-9

5. Auditing and Event Logging **5-1**

5.1 Systemwide Auditing 5-1
5.2 Individual File Auditing 5-3
5.3 Summary of Recommendations 5-4

6. Windows 2000 Professional Installation **6-1**

6.1 Why Choose NTFS? 6-1
6.2 How to Convert Non-NTFS Partitions 6-1
6.3 Other settings 6-2
6.4 Creating and Protecting the ERD 6-2
6.4.1 How to Create an ERD 6-3
6.4.2 How to Protect ERD 6-3
6.4.3 How to Protect ERD Backup 6-4
6.5 Summary of Recommendations 6-5

7. Updating and Patching Guidelines **7-1**

7.1 Windows 2000 Professional Updates 7-1
7.2 Windows 2000 Patching Resources 7-3
7.2.1 Internet Security Portals 7-3
7.2.2 Windows Update Web Site 7-4
7.3 Summary of Recommendations 7-5

8. Windows 2000 Pro Configuration Guidelines 8-1

8.1 Securing the File System Using ACLs 8-1
8.1.1 File System ACL 8-1
8.1.2 Setting ACLs 8-1
8.1.3 ACL Example 8-1
8.1.4 Windows 2000 Access Control 8-2
8.1.5 Replace Default Access Rights 8-3
8.2 Encrypted File System 8-4
8.2.1 How Does EFS Work? 8-4
8.2.2 How Is EFS Implemented? 8-4
8.2.3 EFS Example 8-5
8.2.4 EFS Data Recovery 8-7
8.3 Additional File System Security Measures 8-8
8.3.1 Removal of OS2 and POSIX 8-8
8.3.2 Prevent Data Remnants 8-9
8.4 Securing the Network Interface 8-11
8.4.1 TCP/IP Port Filtering 8-13
8.4.2 IPsec Filtering 8-13
8.5 Disabling Unnecessary Services 8-16
8.5.1 Windows 2000 Professional Services 8-18
8.6 Domain Member Machine Configuration 8-19
8.7 Summary of Recommendations 8-19

9. Administrator, Power Users, and Users 9-1

9.1 Windows 2000 Security Identifier 9-2
9.2 Administrators Group 9-2
9.3 Power Users Group 9-2
9.4 Users Group 9-4
9.5 Change Account Group Membership 9-5
9.6 Account Policies 9-6
9.7 Summary of Recommendations 9-7

10. Application-Specific Configuration 10-1

10.1 AntiVirus Scanners 10-1
10.1.1 McAfee Virus Scan 10-2
10.1.2 Norton AntiVirus 10-5
10.1.3 F-Secure Anti-Virus 10-7
10.2 E-mail Clients 10-9
10.2.1 Microsoft Outlook Security 10-9
10.2.2 Qualcomm Eudora 10-15
10.3 Web Browsers 10-20
10.3.1 Microsoft Internet Explorer 10-20
10.3.2 Netscape Navigator 10-24
10.4 Productivity Applications 10-29
10.4.1 Microsoft Office Installation Issues 10-29
10.4.2 Microsoft Office Updates 10-30
10.4.3 Office 2000 Macro Virus Security 10-30
10.5 Summary of Recommendations 10-32

11. Remote System Seat Management 11-1

11.1 Software Installation AND MAINTENANCE 11-1
11.2 Change and Configuration Management 11-2
11.3 Add-On Management Software 11-2

12. Conclusion 12-1

Appendix A— Registry Discussion A-1

Appendix B— NIST Windows 2000 Security Templates B-1

Appendix C— Tools C-1

Appendix D— Windows XP Security Components Overview D-1

Appendix E— References Used E-1

Appendix F— Other References F-1

Appendix G— Summary of Recommendations G-1

Appendix H— Acronyms H-1

Appendix I— Index I-1

LIST OF FIGURES

Figure 4-1. Open MMC Console 4-2
Figure 4-2. Create New Database 4-3
Figure 4-3. Select Template 4-3
Figure 4-4. Analyze of Current Settings 4-4
Figure 4-5. Change Database Settings 4-4
Figure 4-6. Configure Computer Settings 4-5
Figure 4-7. Windows 2000 Local Computer Security Settings Policy Node 4-7
Figure 4-8. Windows 2000 Local Security Policy Export 4-9
Figure 5-1. Event Viewer 5-1
Figure 5-2. System-Wide Audit Policy 5-2
Figure 5-3. Advanced File Settings 5-3
Figure 5-4. File Auditing 5-4
Figure 6-1. Open Windows 2000 Backup and Recovery Tools 6-3
Figure 6-2. Backup ERD Showing SAM File 6-4
Figure 6-3. Restrict NTFS Permissions for winnt\repair Directory 6-5
Figure 7-1. Windows Update Web Site 7-5
Figure 8-1. ACL for Sample System Partition 8-2
Figure 8-2. Advanced ACL Window for Sample System Partition, Access Control Settings Screen 8-3
Figure 8-3. Advanced ACL window for sample system partition, Permission Entry Screen 8-3
Figure 8-4. Confirm Application of EFS Encryption to Current Resource 8-5
Figure 8-5. Directory Listing with Sample Folder 8-5
Figure 8-6. Advanced Attributes Window for Sample Folder 8-6
Figure 8-7. Updated Directory Listing of Sample Folder 8-6
Figure 8-8. Recovery Agent Default Setting 8-7
Figure 8-9. Updated Folder Listing of Sample Folder 8-9
Figure 8-10. Disable Operating System Memory Dumps 8-10
Figure 8-11. Set Recycle Bin to Auto-Delete All Files 8-11
Figure 8-12. Disable LMHOSTS Lookup and NetBIOS Tunneling 8-12
Figure 8-13. IP Filter List 8-14
Figure 8-14. Source and Destination Address 8-14
Figure 8-15. Mirror Filter Settings 8-15
Figure 8-16. A Sample IPsec Policy 8-16
Figure 8-17. Disable Unnecessary Services 8-17

Figure 9-1. Open Local Users and Groups from Computer Management 9-5
Figure 9-2. Account Properties Box for Example Account Client 9-6
Figure 9-3. Adding a User to a Group 9-6
Figure 9-4. NIST Template Password Policy 9-7
Figure 10-1. Update McAfee Virus Scan 10-3
Figure 10-2. McAfee Virus Scan Update in Progress 10-3
Figure 10-3.Configure McAfee E-mail Scanning 10-4
Figure 10-4.Configure McAfee Settings Password Protection 10-5
Figure 10-5. Set Norton AntiVirus Bloodhound Detection Levels 10-6
Figure 10-6. Set Norton AntiVirus Automatic Live Update 10-7
Figure 10-7. F-Secure Anti-Virus Real-time Options Window 10-8
Figure 10-8. F-Secure Anti-Virus Update Options Window 10-9
Figure 10-9. Windows 2000 Known File Types Window 10-11
Figure 10-10. Change Behavior of Outlook after Interacting with New Message 10-12
Figure 10-11. Set Windows 2000 to Display All Known File Extensions 10-13
Figure 10-12. Set Outlook Attachment Security to High 10-14
Figure 10-13. Set Outlook Security Zone 10-14
Figure 10-14. Set Outlook Macro Security 10-15
Figure 10-15. Eudora.ini Properties File 10-16
Figure 10-16. Choose Where to Install Eudora Data Files 10-17
Figure 10-17. Eudora Default Directory Permissions 10-18
Figure 10-18. Disable Executables in HTML Messages in Eudora 10-19
Figure 10-19. Enable Executable Warnings in Eudora 10-20
Figure 10-20. Disable Scripting in Internet Explorer 10-21
Figure 10-21. Disable Java in Internet Explorer 10-22
Figure 10-22. Set Custom Microsoft JVM Permissions 10-23
Figure 10-23. Confirm Clearing Cache on Internet Explorer 10-24
Figure 10-24. Registry Error Installing Netscape as a Regular User 10-25
Figure 10-25. Netscape Communicator Update Requesting Java Permission 10-26
Figure 10-26. Netscape Signed Java Applet/JavaScript Window 10-27
Figure 10-27. Disable Active Content within Netscape Communicator 10-28
Figure 10-28. Installed Netscape Plugins 10-29
Figure 10-29. Office 2000 Installation Procedure 10-30

LIST OF TABLES

Table 4-1. Secedit Syntax 4-6
Table 4-2. Local Security Policy List 4-8
Table 4-3. Settings for NISTWin2kProGold.inf Security Options 4-8
Table 5-1. Systemwide Audit Policy Description 5-2
Table 7-1. Security Bulletins Included in Service Pack 3 7-2
Table 7-2. Information Security Portals 7-4
Table 8-1. Windows 2000 Professional Services 8-17
Table 9-1. Default Access Control Settings for File System Objects 9-3
Table 10-1. Registry Keys Netscape Cannot Successfully Access During Installation 10-25

Executive Summary

The National Institute for Standards and Technology (NIST) produced the *Systems Administration Guidance for Securing Microsoft Windows 2000 Professional System* to assist personnel responsible for the administration and security of Windows 2000 Professional (Win2K Pro) systems. This guide is intended for *managed environments* and should not be applied throughout an enterprise unless trained and competent systems administrators (SA) are available on the staff. Experienced SAs in these managed environments may use this guide to secure local Win2K Pro workstations, Win2K Pro mobile computers, and Win2K Pro computers used by telecommuters. NIST recommends that users who are directly applying this guide to secure their computers have significant competence in the administration of Windows systems.

The guide provides detailed information about the security features of Win2K Pro, security configuration guidelines for popular applications, and security configuration guidelines for the Win2K Pro operating system. The guide documents the methods that SAs can use to implement each security setting recommended. The principal goal of the document is to recommend and explain tested, secure settings for Win2K Pro workstations with the objective of simplifying the administrative burden of improving the security of Win2K Pro systems.

This guide includes security templates that will enable SAs to apply the security recommendations rapidly. The NIST Windows 2000 Professional Security Templates are text-based configuration files that specify values for security-relevant system settings. The security templates modify several key policy areas of a Windows 2000 Professional system. The policy areas include password policy, account lockout policy, auditing policy, user rights assignment, system security options, event log policy, system service settings, and file permissions.

The NISTWin2kProGold.inf security template development was initially based in part on the National Security Agency's (NSA) Win2K Pro guidance. We examined the NSA settings and guidance and built on the excellent material they developed. NIST conducted extensive analysis and testing of the NSA settings, substantially extended and refined the NSA template settings, and developed additional template settings. NIST developed detailed explanatory material for the template settings, Win2K Pro security configuration, and application specific security configuration guidance. Subsequently, NIST led the development of a consensus baseline of Win2K security settings in collaboration with the public and private sectors; most notably NSA, Defense Information Systems Agency (DISA), the Center for Internet Security (CIS), and the SysAdmin Audit Network Security Institute (SANS). Microsoft also provided valuable technical commentary and advice. The consensus settings are reflected in the NISTWin2kProGold.inf security template.

The development of the NISTWin2kProGoldPlus.inf security template was driven by a need for added restrictions to create a more secure Win2K Pro workstation. The NISTWin2kProGoldPlus.inf security template contains all of the settings of the NISTWin2kProGold.inf security template, plus added restrictions on command line executables that could be used by attackers to gather network information or launch malicious files. Many of the restricted executables may be commonly used by users within an organization. Therefore, use caution when applying the security template and make modifications to the security template application restriction settings to conform to local policy before application.

The NIST security templates can be rapidly applied to a Windows 2000 Professional operating system using the Security Configuration Tool Set or the command line tool Secedit. Every Win2K Pro system includes these configuration tools, which can be used to analyze, configure, export, and verify the security configuration of a Windows 2000 system. The Security Configuration Tool Set is a graphical user interface (GUI) based tool allowing SAs to centrally test and apply security policies for standalone and

domain member Windows 2000 Professional workstations. The Secedit tool is a command line utility that performs the functions of the Security Configuration Tool Set. Secedit is most useful in a workgroup environment without a domain controller, enabling quick deployment of security settings to multiple computers. Either of these tools may be used to apply the NIST Win2K Pro security configuration templates that are included in this guide.

NIST also recommends that organizations —

- Use the **Security Configuration Analysis** snap-in and the **Local Security Policy** tool to import, analyze, modify, configure, and export the security settings for most situations.
- Use the **secedit.exe** tool in a script file to apply security settings to Windows 2000 Professional systems in a workgroup environment.
- Apply the appropriate NIST security configuration template to configure the Security of Windows 2000 Professional systems.
- ***Fully test*** the configuration provided by this guide before wide-scale deployment to ensure not only that the recommended configuration does not contradict local security policy but also that the recommended settings do not interfere with local applications. Some modifications will be needed for legacy applications.

The security configuration guidance provided in this document was built and tested from a clean Windows 2000 Professional installation. NIST recommends that SAs build their systems from a clean formatted state to begin the process of securing Windows 2000 Professional workstations. NIST also recommends that the installation process be performed on a secure network segment or off the organization's network until the security configuration is completed, all patches are applied, and strong passwords are set for any accounts built in or created during the installation.

NIST recommends the following steps in the installation of Windows 2000 Professional Systems:

- Partition the hard drive using the **New Technology File System (NTFS)** for system and data files.
- Install the operating system (OS) with minimum required services.
- Install **Transmission Control Protocol/Internet Protocol (TCP/IP)** networking and **Client for Microsoft Networking** only.
- Secure the **winnt\repair** directory. The NIST security template does this automatically.
- Create an Emergency Repair Disk (ERD) when the security configuration is complete. The ERD is used for disaster recovery.
- Securely store the ERD on removable media.
- Delete or restrict access to the backup ERD located in the **winnt\repair** directory.
- Perform regular backups of installed systems and sensitive data.

After the Windows 2000 Professional OS has been installed and securely configured, it must be regularly monitored and patched when necessary. Windows 2000 Professional users and SAs have two major methods for updating Windows systems: service packs and hotfixes. The Windows service pack, which provides improvements and replacements to OS components, includes all hotfixes that had been released before the service pack cutoff date. Hotfixes are released rapidly when a vulnerability or problem is

discovered within Windows systems or Microsoft applications. Once Microsoft releases a Service pack or hotfix it should be tested thoroughly and applied to systems within an organization at once.

NIST recommends the following steps for patching already installed systems:

- Subscribe to the Microsoft Security mailing list (http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/notify.asp) and other security lists to stay abreast of current threats and vulnerabilities to the Windows 2000 OS and applications.
- Periodically scan systems to determine patch status using the Windows Update Web site (http://windowsupdate.microsoft.com) or the **Microsoft Baseline Security Analyzer** tool (http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/Tools/MBSAhome.asp) provided by Microsoft.
- Use the Microsoft Security site (http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/current. asp) as a portal to search for and download Microsoft security patches.
- Test and apply patches when required.
- Update or create a new ERD after the system has been patched.

This guidance document also includes recommendations for testing and configuring common Windows applications. The application types include electronic mail (e-mail) clients, Web browsers, productivity applications, and antivirus scanners. This list is not intended to be a complete list of applications to install on Windows 2000 Professional, nor does it imply NIST's endorsement of particular commercial off-the-shelf (COTS) products. Many of the configuration recommendations for the tested Windows applications focus on deterring viruses, worms, Trojan horses, and other types of malicious code. The guide presents recommendations to protect the Windows 2000 Professional system from malicious code when the tested applications are being used.

NIST recommends the following steps in the testing and configuration of some common Windows applications:

- Antivirus scanners
  - Do not install two different AntiVirus scanners on the same machine.
  - Ensure that AntiVirus scanners are configured properly and updated periodically (weekly or sooner when a major virus outbreak occurs).
  - Perform a full scan of your system after the virus definition database has been updated.
  - Enable Auto-Protection scanning of new software and documents introduced to your system (all file types).
  - Enable e-mail and Internet scanning.
- E-mail clients
  - Frequently update e-mail clients.
  - Disable Visual Basic Scripting in Microsoft Outlook.

  - Turn off the Outlook preview pane.
  - Display extensions for attachments.
  - Set Outlook's attachment security to HIGH.
  - Set Outlook's Macro Security level to HIGH.
  - Install the Outlook E-mail Security Update (OESU) that blocks receipt of executable attachments, and sending of e-mail by unauthorized programs. (The OESU is integrated in Outlook 2000 Service Pack 2 and in Outlook 2002 for Office XP. The OESU is available as a free download for Outlook 98 and earlier configurations of Outlook 2000.)
  - Secure the user's e-mail data directory.
  - Disable executables in Hypertext Markup Language (HTML) content in Eudora.
  - Deselect the Use Microsoft's viewer option in Eudora.
  - Enable message warnings in Eudora.

- Web browsers
  - Frequently update Web browsers.
  - Upgrade encryption level to 128 bits.
  - Disable Active Scripting if your organization requires a high level of security. **Note:** Disabling ActiveX will prevent Microsoft's Windows update site and many other Web sites from working properly. If Service Pack 3 and the included Automatic Update feature are installed, however, automatic updates will still work without Active Scripting. Thus, consideration of selectively enabling and disenabling certain ActiveX functionality may be required to operate certain key features.

- Office 2000 productivity applications
  - Frequently update Office 2000 applications by going to http://office.microsoft.com/ProductUpdates/default.aspx.
  - Set macro security level to HIGH.
  - Digitally Sign safe macros used within your environment.
  - Enforce installed Add-ins with the same security requirements as opening documents.
  - Protect temporary files created by Office 2000 applications.

The *Systems Administration Guidance for Securing Microsoft Windows 2000 Professional System* provides recommendations to assist organizations in making their Windows 2000 Professional OSs more secure. The settings and recommendations provide SAs with the information necessary to modify the settings and to comply with local policy or special situations. The recommendations and settings provide a high level of security for all Windows 2000 Professional systems when used in conjunction with a sound and comprehensive local security policy and other relevant security countermeasures. The guidelines are also appropriate for managed environments that are configuring and deploying laptops for mobile users and desktop computers for telecommuters.

1. Introduction

Windows 2000 Professional has many valuable security features System Administrators (SA) can enable to protect their users and their Network. This document concentrates on simplifying the various security settings Windows 2000 Professional has to offer. The document examines the security registry settings and the recommended security settings for Windows 2000 Professional and selected applications.

Users and SAs will be able to familiarize themselves with the full security and usability impact of Windows 2000 Professional settings so that they can make educated decisions about what should be applied within their environment. Additionally, a large reference of books and security sites, brief overviews of Remote Systems Management, and Windows XP's security features are included to assist with further research and education.

Two security templates have been developed and tested, fully documented, and included with this document to assist SAs in implementing security on their domain member and stand-alone Windows 2000 Professional workstations. These templates can be applied with the Microsoft's Security Configuration Tool Set. The templates are explained in this document and commented internally. The security templates were based on the templates and guidance released by the National Security Agency (NSA) for Windows 2000 and other recommended practice documents released by the security community.

1.1 Authority

This document has been developed by the National Institute of Standards and Technology (NIST) in furtherance of its statutory responsibilities under the Computer Security Act of 1987[1] and the Information Technology Management Reform Act of 1996, specifically 15 United States Code (U.S.C.) 278 g-3 (a)(5). This document is not a guideline within the meaning of 15 U.S.C 278 g-3 (a)(3).

These guidelines are for use by federal organizations that process sensitive information. They are consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Appendix III.

This document may be used by nongovernmental organizations on a voluntary basis. It is not subject to copyright. Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding upon federal agencies by the Secretary of Commerce under his statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, the Director of the OMB, or any other federal official.

1.2 Purpose and Scope

This guide is intended to assist SAs in securing Win2K Pro workstations, Win2K Pro mobile computers, and Win2K Pro computers used by telecommuters within *managed environments* and should not be applied throughout an enterprise unless trained and competent SAs are available on the staff. NIST recommends that users who are directly applying this guide to secure their computers have significant competence in the administration of Windows based systems.

[1] The Computer Security Act provides a broad definition of the term "sensitive information"— namely "any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy."

The guide provides detailed information about the security features of Win2K Pro, security configuration guidelines for popular applications, and security configuration guidelines for the Win2K Pro operating system. The guide documents the methods that SAs can use to implement each security setting recommended. The principal goal of the document is to recommend and explain tested, secure settings for Win2K Pro workstations with the objective of simplifying the administrative burden of improving the security of Win2K Pro systems.

1.3 Objective

The objective of this document is to provide guidance and recommended practices for installing, configuring, and securing Windows 2000 operating systems and popular applications.

1.4 Audience And Assumptions

The intended audience is composed of Windows 2000 Systems Administrators and technical Windows 2000 Professional users. The document assumes that the reader has some experience installing and administering Windows-based systems in domain or stand-alone configurations. The document discusses in technical detail the various Windows 2000 Professional security registry and application settings.

1.5 Document Structure

This document is divided into 12 sections followed by 9 appendices. This subsection describes the structure of the document.

- Section 1 (this section) provides an introduction, authority, purpose and scope, objective, audience and assumptions, and document structure.
- Section 2 gives the reader a review of security components offered in the Windows 2000 Professional system.
- Section 3 explains the differences between a Windows stand-alone workstation and a domain member.
- Section 4 explains the use of the Security Configuration Tool Set.
- Section 5 presents Windows 2000 Professional security auditing.
- Section 6 covers Windows 2000 Professional installation recommendations.
- Section 7 presents Updating and Patching Guidelines for Windows 2000 Professional workstations.
- Section 8 demonstrates how to apply recommended security settings on Windows 2000 Professional systems.
- Section 9 presents recommendations for user, administrator, and power user built-in groups.
- Section 10 demonstrates securing popular antivirus programs, e-mail clients, Web browsers, and Microsoft Office applications.
- Section 11 discusses how the Intel LanDesk and Systems Management Server (SMS) can be used to enhance Windows 2000 Professional security.
- Section 12, the summary, provides a brief review of the document.

- Appendix A presents an overview, extended discussion of the Windows 2000 registry, and specific keys modified by the NIST template.
- Appendix B contains the detailed registry keys and security settings modified by the NIST security templates. The current version of the Appendix B and accompanying templates can be downloaded from the following page: http://csrc.nist.gov/itsec/guidance_W2Kpro.html
- Appendix C lists some useful administration tools.
- Appendix D discusses some security components offered in Windows XP.
- Appendix E lists references used in this document.
- Appendix F lists other references to assist SAs with further research and education.
- Appendix G provides a checklist of all the recommendations.
- Appendix H lists acronyms used in the document.
- Appendix I contains the index table.

This page intentionally left blank

2. Windows 2000 Security Components Overview

This section presents the various security components offered by the Windows 2000 Professional operating system (OS). These new security features include network authentication with Kerberos version 5, integrated personal computer/smart card (PC/SC) version 1.0 compliant smart card logon support; enhanced public key infrastructure (PKI) support, including X509 version 3 certificates and X500 directory services Certificate Revocation List (CRL) version 2; native IP Security (IPsec) support provided by Windows IP Security; support for Point-to-Point Tunneling Protocol (PPTP) and Layer Two Transport Protocol (L2TP) for virtual private network (VPN) services; and support for Encrypted File System (EFS).

EFS and simple IPsec filters are the only technologies that will be covered in detail within this document. The additional security technologies described in Section 2 require configuration within the active directory of the Windows 2000 server and fall outside the scope of this document.

2.1 Kerberos Support

In a domain configuration, Windows 2000 provides support for MIT Kerberos v.5 authentication, as defined in Internet Engineering Task Force (IETF) Request for Comment (RFC) 1510. The Kerberos protocol is composed of three subprotocols: Authentication Service (AS) Exchange, Ticket-Granting Service (TGS) Exchange, and Client/server (CS) Exchange. The Kerberos v.5 standard can be used only in pure Windows 2000 domain environments. For a more detailed explanation of how Kerberos works in a Windows 2000 domain environment, refer to http://support.microsoft.com/support/kb/articles/Q217/0/98.ASP.

Windows 2000 domain members will use Kerberos as the default network client/server authentication protocol, replacing the older LanManager (LM) and Windows NT LanManager (NTLM) authentication methods. The older methods are still supported to allow legacy Windows clients to authenticate to a Windows 2000 domain environment. Windows 2000 Professional stand-alone workstations and members of NT domains do not use Kerberos to perform local authentication; they use the traditional NTLM. For Windows 2000 domain members Kerberos provides the following benefits:

- **Efficiency.** Kerberos provides a client with credentials that eliminate the need for intermediary application servers in the authentication process.
- **Improved Authentication Trust Management.** Trust relationships in Kerberos have been improved to have finer controls and can be two-way and transitive.
- **Interoperability.** The Windows 2000 Kerberos implementation is interoperable with other v.5 implementations of Kerberos clients.

2.2 Smart Card Logon Support

In the past, interactive logon meant an ability to authenticate a user to a network by using a form of a shared credential, such as a hashed password. Windows 2000 supports public-key interactive logon by using a X.509 v.3 certificate stored on a smart card. Instead of a password, the user types a personal identification number (PIN) to the graphical identification and authentication (GINA), and the PIN authenticates the user to the card. Windows 2000 Smart card authentication can be used to log on only to domain accounts, not local accounts.

The user's public key certificate is retrieved from the card through a secure process and verified to be valid and from a trusted issuer. During the authentication process, a challenge based on the public key contained in the certificate is issued to the card.

After successful verification of the public-private key pair, the user's identity contained in the certificate is used to reference the user object stored in the active directory to build a token and return a Ticket-Granting Ticket (TGT) to the client. Public key logon has been fully integrated with the Microsoft implementation of Kerberos v.5.

2.3 PKI Support

The PKI support within Windows 2000 extends beyond the public key services that have been available to previous Windows environments. The PKI support that Microsoft integrated into Windows 2000 affects many core security functions of the OS. At the client level, the Microsoft cryptographic service provider within Windows 2000 Professional and server, called CryptoAPI, has been extended to provide support for X509 v.3 public key certificates and to provide compatibility with CRL v.2 standard. As stated previously, this technology integrates with the smart card support and VPN and IPsec services within Windows 2000 to allow for several types of strong authentication.

2.4 IPsec Support

Windows 2000 includes an implementation of the IETF IPsec standard called Windows IP Security. Windows IP Security simplifies deployment and management of network security and supports network-level authentication, data integrity, and encryption. The benefits of Windows 2000 IPsec are as follows:

- **Authentication.** Strong authentication services prevent the interception of data by using falsely claimed credentials.
- **Confidentiality.** Confidentiality services prevent unauthorized access to sensitive data as it passes between communicating parties.
- **Data Integrity.** IP authentication headers and variations of hash message authentication code ensure data integrity during communications.
- **Dynamic Rekeying.** Dynamic rekey during ongoing communications helps protect against attacks.
- **Secure Links End to End.** Windows IPsec provides secure links end to end for private network users within the same domain or across any trusted domain in the enterprise.
- **Centralized Management.** Network administrators use security policies and filters to provide appropriate levels of security, based on user, work group, or other criteria. Centralized management reduces administrative overhead costs.
- **Standalone Workstations.** IPsec can be configured to work with nondomain member workstations using custom policies with pre-shared secrets or certificates. For further information about this method, visit the following Web page: http://www.microsoft.com/windows2000/techinfo/planning/security/ipsecsteps.asp
- **Access Control List Filters.** IPsec filter lists can be used to provide some level of access control based on the source and destination of the Transmission Control Protocol/Internet Protocol (TCP/IP) packets.

2.5 PPTP And L2TP Support

The PPTP and L2TP are VPN remote access technologies that can be used to create a secure reliable communications channel between two endpoints. PPTP enables the secure transfer of data from a remote computer to a private server by creating a VPN across TCP/IP-based data networks. L2TP uses Windows 2000's implementation of IPsec, Windows IPsec, to provide authentication and encryption to protect data in transit over untrusted communications channels. PPTP and L2TP support on-demand, multiprotocol, virtual private networking over public networks, such as the Internet. The Windows 2000 implementation of L2TP does not support native tunneling over X.25, Frame Relay, or asynchronous transfer mode (ATM) networks.

2.6 Encrypting File System Support

The encrypting filing system (EFS) is a new Windows 2000 feature providing file system level security by allowing users to transparently encrypt or decrypt files and folders residing on a Windows 2000 New Technology File System (NTFS) partition. EFS uses the Expanded Data Encryption Standard (DESX) algorithm, a variant of the Data Encryption Standard (DES), by installing Service Pack 2 and higher or the high encryption pack.

EFS maintains encryption persistence, meaning that any file or folder that has been designated as encrypted will remain encrypted when moved. EFS will automatically decrypt a file only if the encrypted resource is moved by the file owner to a partition not formatted as NTFS.

This page intentionally left blank

3. Stand-Alone Versus Domain Member

This document focuses on two distinct configurations of Windows 2000 Professional workstation: Stand-Alone and Domain Member. Each configuration has unique advantages and disadvantages.

3.1 Stand-Alone

The Windows 2000 Professional Stand-alone configuration is widely deployed in homes and small organizations. In this configuration, each networked Windows machine belongs to a workgroup of one or more machines. The authentication for the resources (e.g., printer, files) contained on the workstation is performed on the workstation using the local Security Accounts Manager (SAM). If users require remote access to the resources contained on the Windows 2000 Professional Stand-alone workstation, they must authenticate directly to that machine. Every user who must have access to resources on the machine must have an account on the machine's local SAM. For example, a user in a workgroup needs access to resources on five other machines within his or her organization; the user must have a user id and password on each machine.

Each computer in a stand-alone (workgroup) configuration must be managed individually. Windows 2000 provides no built-in options for the centralized management of multiple workgroup computers. Therefore, each Windows 2000 Professional stand-alone computer requires more time and resources, per machine, to manage than domain member machines.

3.2 Domain

The Windows 2000 Professional Domain Member configuration is widely deployed in medium to large organizations. In this configuration, the Windows 2000 Professional workstation resides within the Windows 2000 domain model. A domain represents a namespace that corresponds to a DNS domain. The first domain created in a Windows 2000 deployment is called the root domain; it is the root of all other domains created in the domain tree. Domain structures in Windows 2000 follow DNS very closely; for example, if company.com is the root domain, hr.company.com could be the name of an additional domain created in the root domain tree.

The basic idea behind the Windows 2000 domain model is to allow logical partitioning. Windows 2000 allows for the existence of multiple domains to simplify management tasks. These multiple domains reside under a common umbrella (root domain). This collection of Windows 2000 domains under a common root (contiguous namespace) is called a tree.

For even larger organizations, Windows 2000 provides a structure called a forest. A forest is a collection of noncontiguous namespaces with transitive trusts existing under the same organization. A forest is a collection of trees.

The primary function of Active Directory services is to catalog all objects residing within the forest. Objects are entities such as a file, folder, printer, user, or computer system that are described by a distinct set of named attributes. The Active Directory uses Organizational Units (OU) to assist SAs by allowing objects to be logically grouped together by, for example, function, OS version, or division to further simplify management, provide updates, and set administrative boundaries.

OUs allow SAs to create administrative and functional boundaries. Using these boundaries, Windows 2000 Professional workstations and users can be centrally managed. Security policy, new software deployment, software updating, security patching, and all user aspects can be managed from a central location.

The Active Directory domain configuration gives SAs maximum control over the security environment of the Windows 2000 Professional workstations within the domain. Connecting to a Windows 2000 domain also allows Windows 2000 Professional workstations to take advantage of many security features not available on stand-alone workstations, such as single sign-on with smart cards and Kerberos.

The scope of this document does not cover the Windows 2000 Server and Active Directory. The above information provided a very basic understanding of the Windows 2000 domain environment. For more information about Windows 2000 Server, Active Directory, OUs, and domains, please refer to http://www.microsoft.com/technet and search on Active Directory.

4. Security Configuration Tool Set

The Windows 2000 Professional system includes the Security Configuration Tool Set. This tool set provides SAs with a centralized location to test and apply security policies for stand-alone and domain member Windows 2000 Professional systems. Use of the Security Configuration Tool Set and Secedit command line interface is presented below. This document provides customized security templates for use with the Security Configuration Tool Set or Secedit. These templates are described in Appendix B.

4.1 Windows 2000 Security Templates

Windows 2000 security templates are text-based files that declaratively specify values for security-relevant system settings. These templates are used by components of the Security Configuration Tool Set components to analyze current security settings or to facilitate the rapid deployment of security settings across a Windows 2000 environment. The templates can be modified using the Microsoft Management Console (MMC) snap-in, called the Security Configuration Editor, to satisfy the specific requirements of unique sites and can be saved for future use in the environment. The templates can also be imported from other locations, such as the templates provided by this document in Appendix B. Windows 2000 also ships with several default security templates that can be used in a Windows 2000 environment. The file name structure for the Microsoft included templates is as follows:
<Security level><operating system class level>.inf

The **<security level>** denotes the security level that will be achieved when the template is applied using Secedit or the Security Configuration Manager MMC snap-in. The possible choices are basic, secure, and hisec (which denotes high security). The **<operating system class level>** indicates what OS the template is for. The possible choices include **ws**, which denotes workstation, and **sv**, which denotes server. Thus, the security template used to apply high security to a standard Windows 2000 Professional installation is named **hisecws.inf**.

The default security templates, **basicwk.inf**, **compatws.inf**, **securews.inf,** and **hsecws.inf**, which are included with Windows 2000, are located in the **%SystemRoot%\security \templates** folder on the **%SystemRoot%** partition. For a description of the Microsoft default security templates, refer to the following article from the SANS organization:
http://www.sans.org/infosecFAQ/win2000/template.htm

Appendix B contains (National Institute of Standards and Technology) NIST Win 2K Pro security templates based on the National Security Agency (NSA) Windows 2000 security templates and recommendations. The included templates have been customized and fully documented for use on Windows 2000 Professional stand-alone and domain member workstations. The **NISTWin2kProGold.inf** security template follows the consensus recommendations of various government and commercial agencies. The **NISTWin2kProGoldPlus.inf** implements all of the security settings included in the **NISTWin2kProGold.inf** security template, plus additional restrictions placed on command line utilities that can be used by attackers to gather network information or launch malicious files. In most cases the **NISTWin2kProGold.inf** template will fully satisfy local policy security requirements. But, for sites that require a slightly more restrictive and secure user environment the **NISTWin2kProGoldPlus.inf** security template. Use caution when applying either of the NIST security templates and if necessary modify them to conform to local security policy. From this point forward the NIST templates will be referred to as NISTWin2kProGold.inf unless a distinction between the two templates is required.

Section 4.4 provides an example for applying templates, using Secedit, to a Windows 2000 Professional installation. This process can be considered a viable alternative to using the Security Configuration Tool Set MMC snap-ins to implement the same security options.

4.2 Analysis and Configuration

This section discusses the analysis and configuration of a Windows 2000 Professional Workstation using the Security Configuration and Analysis Snap-in. The snap-in can compare the current security settings of the workstation to preconfigured templates before they are applied. This action enables SAs to examine the changes the security template will make to the computers settings before they are applied. Start the MMC by using the **Start** menu **Run** command, and open **mmc.exe**. Add the **Security Templates** snap-in and the **Security Configuration and Analysis** snap-in to the MMC. As shown in Figure 4-1, select **Console | Add/Remove Snap-in menu**. When completed, save the console in your **Administrative Tools** folder for future use.

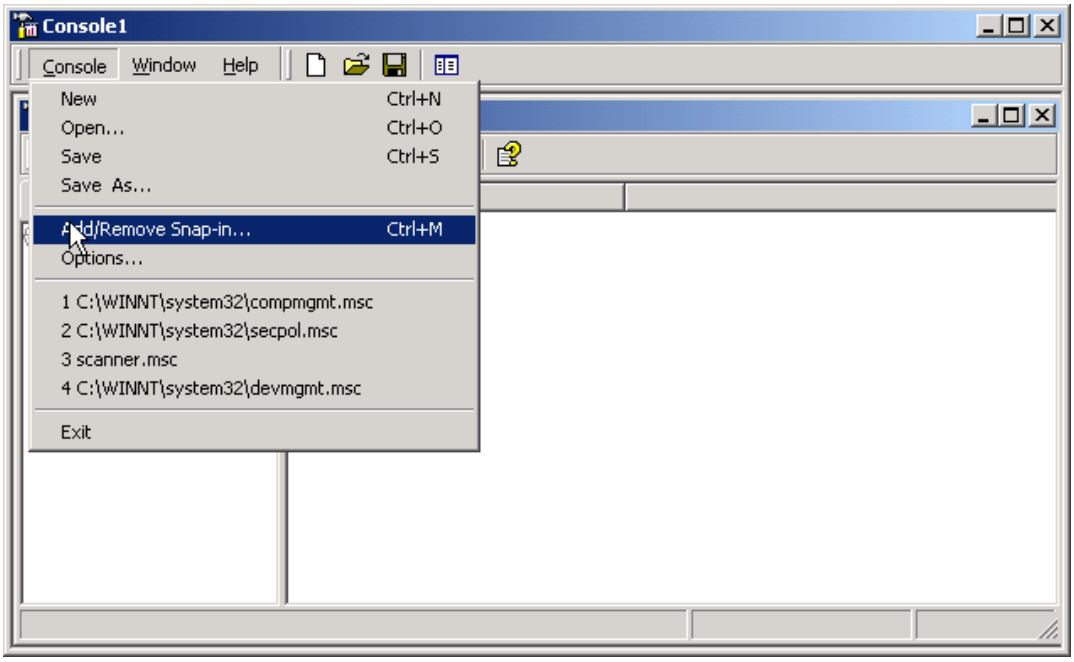

Figure 4-1. Open MMC Console

To use the NIST templates supplied with this document, copy them into the **%SystemRoot%\Security\Templates**[1] folder. Open a new database by right clicking **Security Configuration and Analysis** and selecting **open database**. Name the database and click open, as shown in Figure 4-2.

[1] %SystemRoot% - refers to the WINNT directory located on the system drive (i.e. C:\).

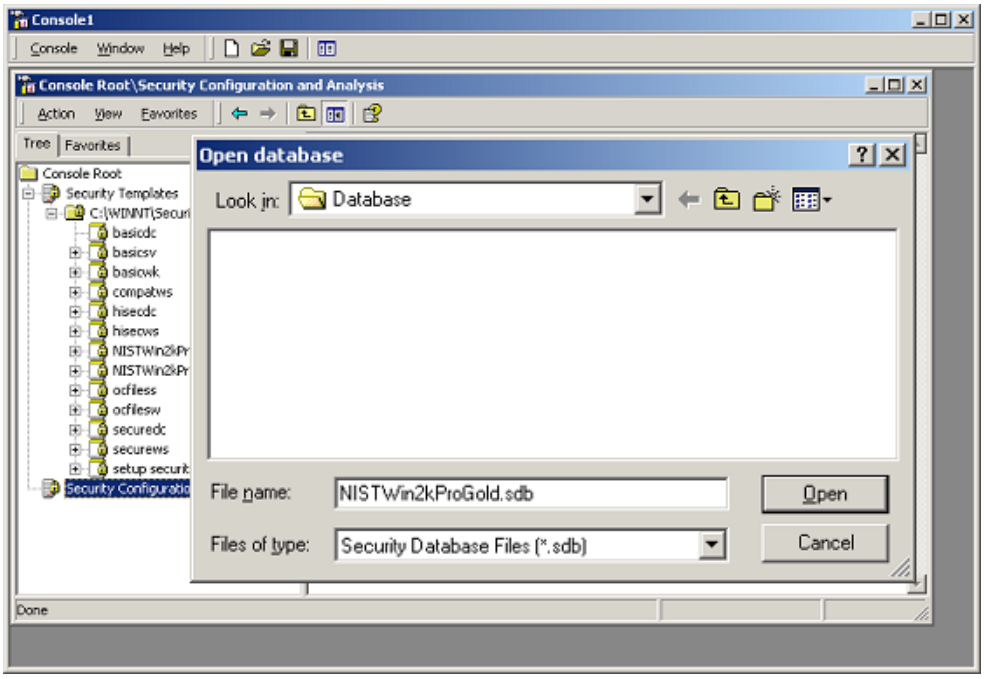

Figure 4-2. Create New Database

Choose the template that will be applied to the workstation, NISTWin2kProGold.inf or NISTWin2kProGoldPlus.inf. Click **Open** to load the setting file, as shown in Figure 4-3.

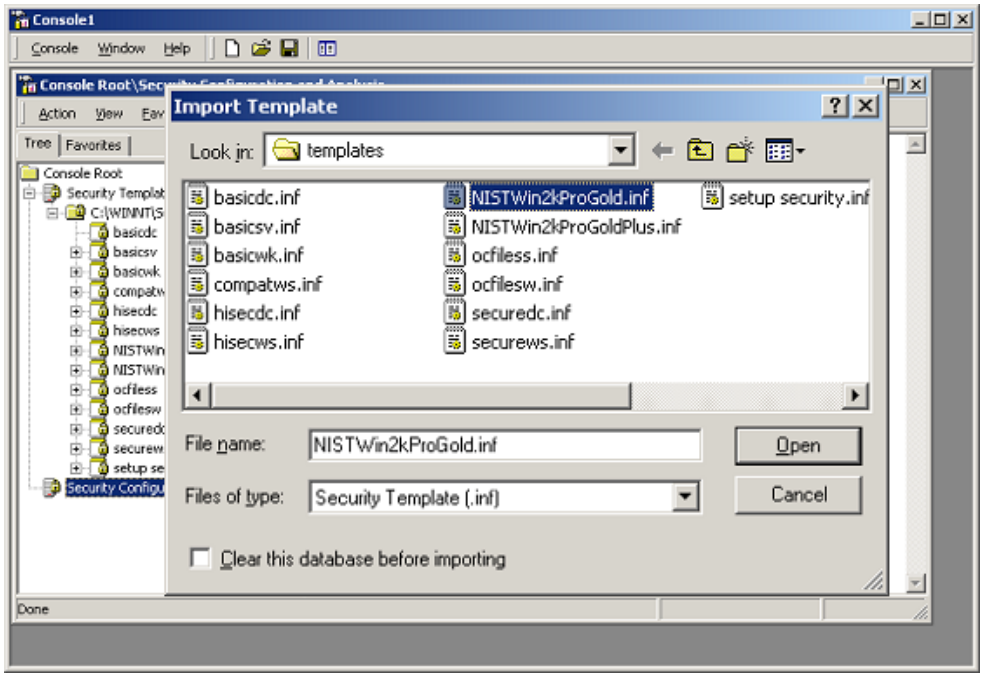

Figure 4-3. Select Template

Right-click the **Security Configuration and Analysis** snap-in and choose **Analyze Computer Now** and the default log name to analyze the current security settings active on the computer.

Seven categories of settings are listed under the Security Configuration and Analysis snap-in. Browse through these settings to view the differences between the templates and the computer configuration. Areas containing a red X differ from the template areas with a green checkmark match the template. Areas with neither a checkmark nor an X mean that the local computer setting is not defined in the template; see Figure 4-4 for an example.

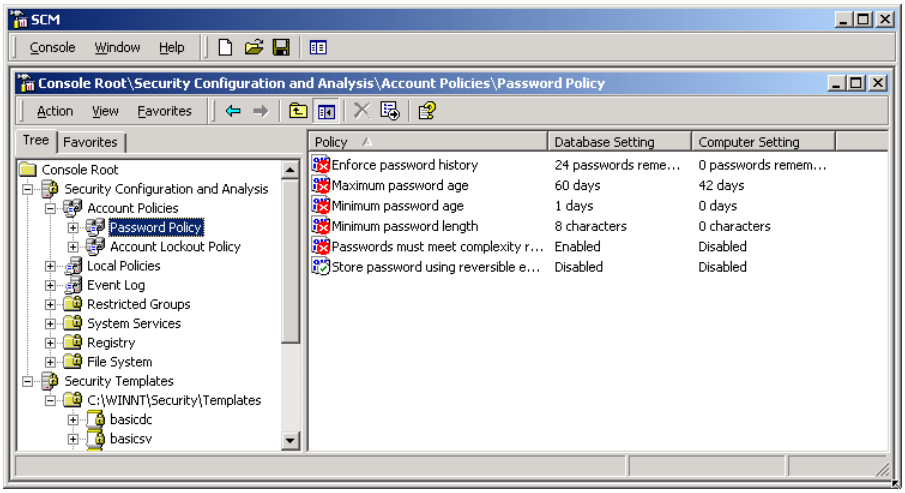

Figure 4-4. Analyze of Current Settings

If the reviewed settings need modification to match settings specific to the environment in which the computer resides, they can be changed by clicking on the policy setting displayed in the analysis window, or the template itself can be changed. NIST recommends that modification of the original templates be avoided. Modify the database or a backup copy of the template. An example of changing the database setting is contained in Figure 4-5.

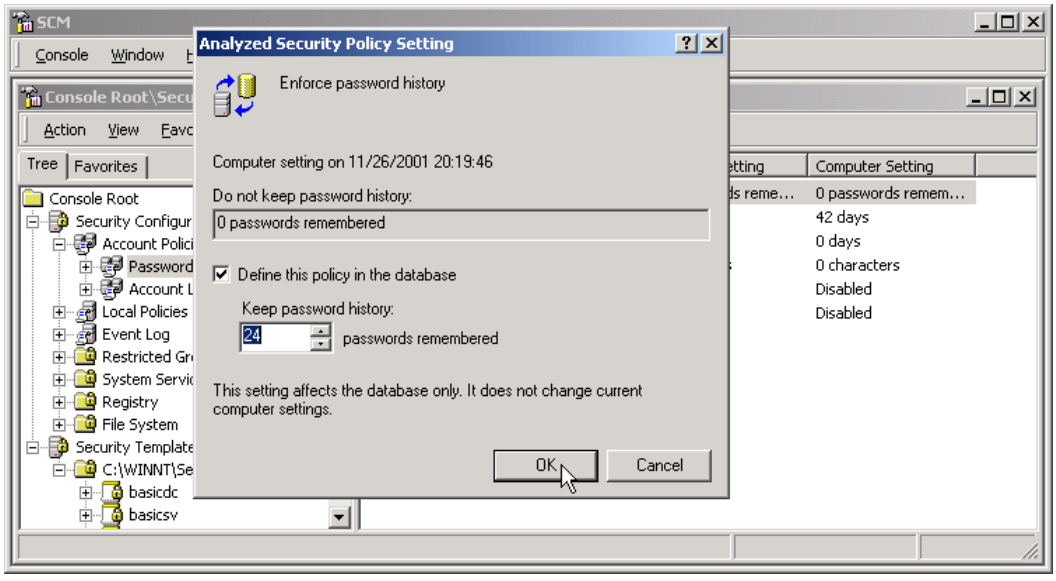

Figure 4-5. Change Database Settings

After all required changed are made to the database, the settings can be applied. The application of the settings is made by right-clicking on the **Security Configuration and Analysis** snap-in and choosing

Configure Computer Now as shown in Figure 4-6. Then, choose the default log location, and the computer configuration is performed.

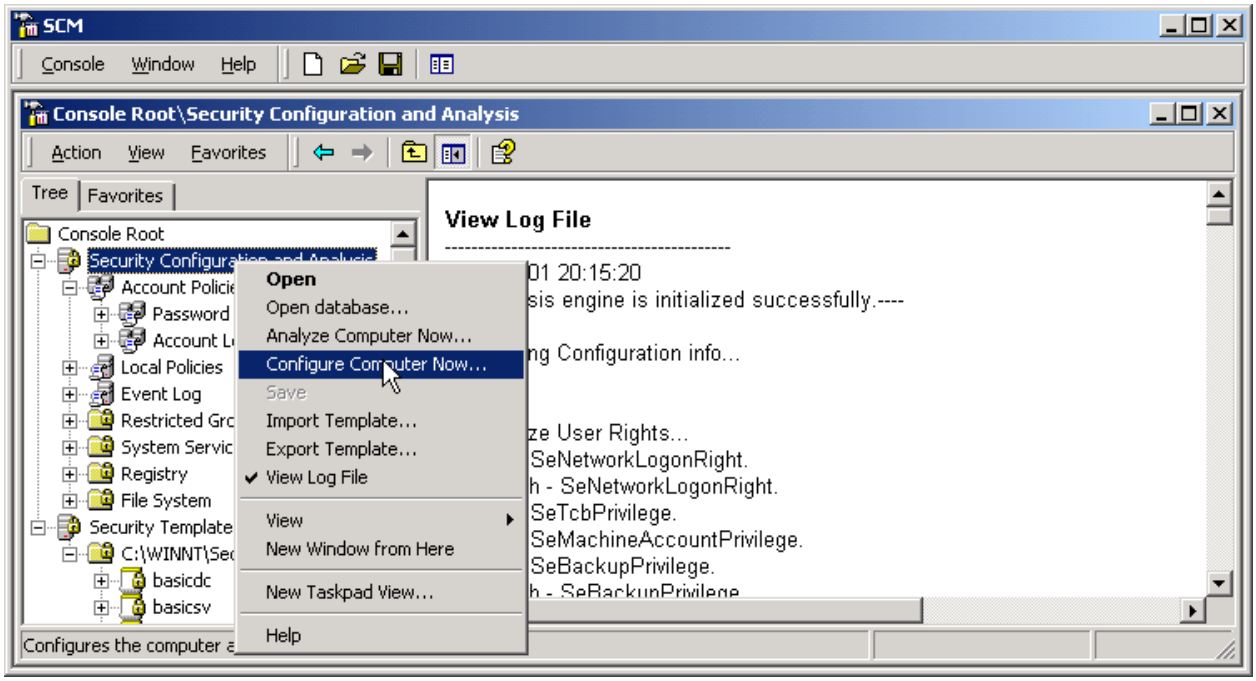

Figure 4-6. Configure Computer Settings

When the computer configuration is completed, the policy used to apply the configuration can be exported for future use on this computer or others. Export the configuration policy by right-clicking on the **Security Configuration and Analysis** snap-in and choosing **Export Template**. Name and save the template for future use on the local computer or other computers in the environment. The saved template file can also be imported to reset settings to a working configuration if future modification is performed and problems arise.

4.3 Group Policy Distribution

In a Windows 2000 Domain environment Group Policy Objects can be used to distribute security settings to all computers in an Active Directory OU. The recommended method of use is to separate computers by role into OUs. For example, all similarly configured domain member workstations within an environment should be in an OU. When a template is fully tested and confirmed to run on computers within an OU, it can be quickly applied to all of the computers in the OU using the Group Policy Editor.

- Select the **Group Policy Object** linked to the OU containing the computers needing the security policy modification.
- Expand **Computer Settings | Windows Settings.**
- Right click **Security Settings** and choose **Import Policy**.
- Select the Template file configured and tested earlier for application on the OU.

The security settings in the template will now be deployed to all computers within the OU. Group Policy can be applied only using a Windows 2000 Server (domain controller) in a Windows 2000 domain

environment (Active Directory). For more information about Active Directory and Group Policy, refer to www.microsoft.com/technet and search on Group Policy.

4.4 Secedit

Secedit is a command line utility that allows a user to perform many of the functions of the Security Configuration Tool Set. Specifically, Secedit is used to analyze, configure, export, and verify the security configuration of a Windows 2000 system. Secedit is most useful in a workgroup environment without a domain controller to quickly deploy security settings to multiple computers.

4.4.1 Secedit Syntax

As stated in Section 1, Introduction, **Secedit.exe** is accessed from the Windows 2000 Professional command prompt. Executing Secedit consists of a supplying action and a series of one or more parameters for each action. Table 4-1 lists possible switches that can be used with the **secedit** command.

4.4.2 Secedit Advantages

Because Secedit is a command line base tool, it can be applied in a scripted manner. When secedit.exe is applied from a logon script, this action automates the need for a network administrator to visit each machine to apply security settings. The information for Secedit.exe has been presented in this document to assist SAs and advanced users in charge of workgroup environments that may not have a Windows 2000 domain controller. Scripting Secedit.exe is the recommended method for securing multiple machines without a domain controller in the environment. The most efficient method of securing Windows 2000 professional machines in a domain environment is to use the Security Settings Extension to the Group Policy Editor to push a group policy object (GPO) security policy from the domain controller to each client workstation attached to the domain. (This method was discussed in Section 4.3.)

4.5 Creating Security Templates

Windows 2000 Professional users are able to create their own security templates. The Security Configuration and Analysis and the Local Security Policy snap-in can be used to create a policy. The first method is described in Section 4.2. This method uses a template as a basis for the configuration and provides a way to export and save the template for use on other computers. Using this method with the Security Templates snap-in, the templates can be directly modified, created, and exported. The secondary method is to create the template by configuring and exporting settings on a computer using the Local Security Policy snap-in. When all of the settings are defined, they can be exported into a template file and then distributed to computers within the enterprise, just as in the first method.

Table 4-1. Secedit Syntax

Syntax	Description
Secedit/analyze	Analyzes system security.
Secedit/configure	Configures system security by applying a security template.
Secedit/export	Exports a stored template from a security database to a security template file.
Secedit/validate filename	Validates the syntax of a security template.

Syntax	Description
Options	**/MergedPolicy**—merges and exports both domain and local policy settings. **/DB filename**—contains the filename and path to the database that contains the security template to be applied. **/CFG filename**—used with the /DB parameter. It specifies which security template will be imported into the database and applied to the user's system. **/overwrite**—used with the /CFG parameter. It tells the Secedit command to overwrite any security template stored in the specified database with the security template specified in the /CFG parameter. **/areas area1 area2**—correspond with the following security policy categories: SECURITYPOLICY, GROUP_MGMT, USER_RIGHTS, REGKEYS, FILESTORE, and SERVICES. **/Log logpath**—contains the path to the log file created during the analysis. **/verbose**—provides detailed progress information during the analysis. **/quiet**—suppresses the screen and log output.

To configure security settings manually, start the **Local Security Policy** found in the **Administrative Tools** folder from the **Control Panel**. This action allows direct access to the Windows 2000 Local Computer Security Settings Policy node, as shown in Figure 4-7. The node also can be accessed by starting the **MMC** and loading the GPO snap-in and choosing the **Local Computer** to manage.

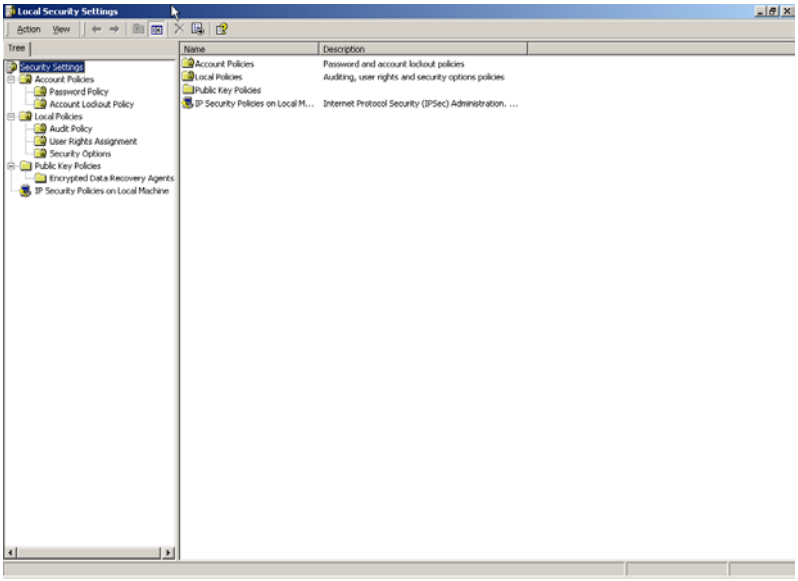

Figure 4-7. Windows 2000 Local Computer Security Settings Policy Node

The Local Security Settings node allows modification of the policy categories listed in Table 4-2.

Table 4-2. Local Security Policy List

Policy	Description
Account Policies	Password policies, account lockout policies, and Kerberos policies
Local Policies	Audit Policy, User Rights Assignment, Security Options

Table 4-3 lists the Policy Description and the Settings within the Security Options section of Local Policies configured by the **NISTWin2kProGold.inf** template to provide an example of the various configuration choices provided by the Local Security Settings Policy Editor. Each policy can be modified to allow conformance to local written security policies and the unique requirements of a network. For example, the **Message text for users attempting to Log on** policy can be configured to the Banner defined by the local written security policy. A full description of all the settings within the Local Security Settings Node and their various configuration options can be reviewed at http://www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp?url=/WINDOWS2000/techinfo/reskit/en-us/gp/615.asp

Table 4-3. Settings for NISTWin2kProGold.inf Security Options

Policy Description	Setting
Additional restrictions for anonymous connections	No access without explicit anonymous permissions
Allow server operators to schedule tasks (domain controllers only)	Not defined
Allow system to be shut down without having to log on	Disabled
Allowed to eject removable NTFS media	Administrators
Amount of idle time required before disconnecting session	30 minutes
Audit the access of global system objects	Enabled
Audit use of Backup and Restore privilege	Enabled
Automatically log off users when logon time expires (local)	Enabled
Clear virtual memory pagefile when system shuts down **Note:** This setting should be enabled or disabled according to your organizational security policy.	Enabled
Digitally sign client communication (always)	Disabled
Digitally sign client communication (when possible)	Enabled
Digitally sign server communication (always)	Disabled
Digitally sign server communication (when possible)	Enabled
Disable CTRL+ALT+DEL requirement for logon	Disabled
Do not display last user name in logon screen	Enabled
LAN Manager Authentication Level	Send NTLMv2 response only\refuse LM & NTLM
Message text for users attempting to log on	
Message title for users attempting to log on	
Number of previous logons to cache (in case domain controller is unavailable) **Note:** Set this value to the number of users using the system on a regular basis if you require domain logon functionality, even when the domain controller is down	1 logon
Prevent system maintenance of computer account password	Disabled

Prevent users from installing printer drivers	Enabled
Prompt user to change password before expiration	14 days
Recovery console: Allow automatic administrative logon	Disabled
Recovery console: Allow floppy copy and access to all drives and all folders	Disabled
Rename administrator account	Not defined
Rename guest account	Not defined
Restrict compact disk—read only memory (CD-ROM) access to locally logged-on user only	Enabled
Restrict floppy access to locally logged-on user only	Enabled
Secure channel: Digitally encrypt or sign secure channel data (always)	Disabled
Secure channel: Digitally encrypt secure channel data (when possible)	Enabled
Secure channel: Digitally sign secure channel data (when possible)	Enabled
Secure channel: Require strong (Windows 2000 or later) session key	Disabled
Send unencrypted password to connect to third-party Server Message Block (SMB) servers	Disabled
Shut down system immediately if unable to log security audits	Enabled
Smart card removal behavior	Lock workstation
Strengthen default permissions of global system objects (e.g., Symbolic Links)	Enabled
Unsigned driver installation behavior	Warn but allow installation
Unsigned nondriver installation behavior	Warn but allow installation

After the desired security options are configured, they can be exported to a template file by clicking on the **Action Menu | Export Policy | Local Policy** and choosing a name for the exported template. The **Export Policy** menu option can be reached from the **Action** menu option, as in the example Figure 4-8. The exported policy can then be deployed to various computers within the enterprise.

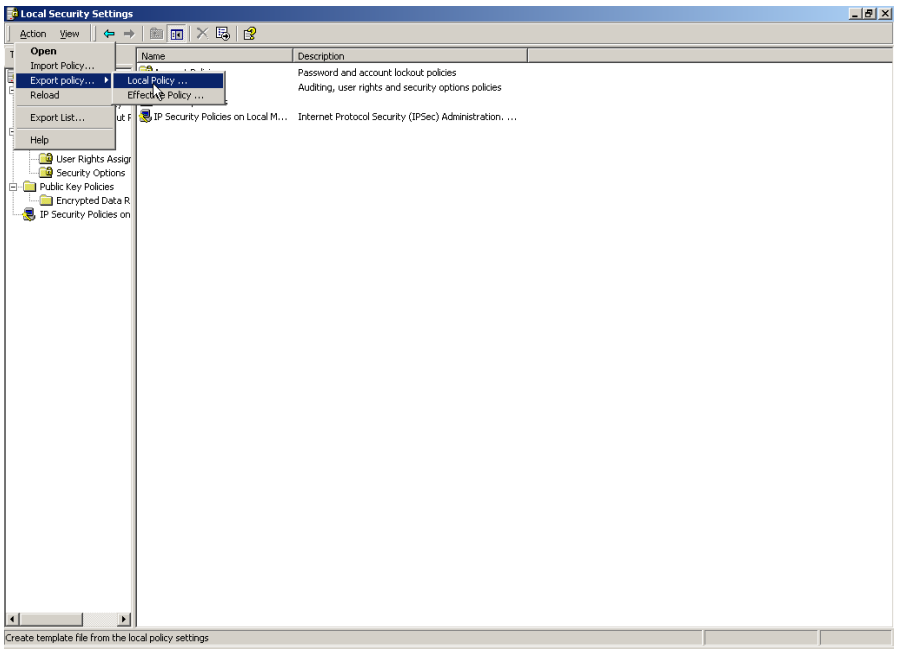

Figure 4-8. Windows 2000 Local Security Policy Export

4.6 Summary of Recommendations

- Use the **Security Configuration Analysis** snap-in and the **Local Security Policy** tool to import, analyze, modify, configure, and export the security settings.

- Use the **GPO** to automate the deployment of security settings to domain member systems.
- Use the **secedit.exe** tool in a script file to apply security settings to the Windows 2000 systems.
- Apply the NIST template to configure the security options.

5. Auditing and Event Logging

Windows 2000 Professional includes powerful auditing capabilities. Windows 2000 Professional performs systemwide auditing of logon events, account management, directory service access, object access, policy change, privilege use, process tracking, and system events. Individual files in the NTFS file system can also be audited. Windows 2000 Professional includes a built-in MMC snap-in tool **Event Viewer** for reviewing of the file and system logs. This tool can be accessed by going to the **Start** menu and choosing **Control Panel | Administrative Tools | Computer Management**. The **Event Viewer** can be accessed under **System Tools** within the **Computer Management MMC** as shown in Figure 5-1. The specific security settings for the Event log as defined by the NIST template can be reviewed in Appendix B.

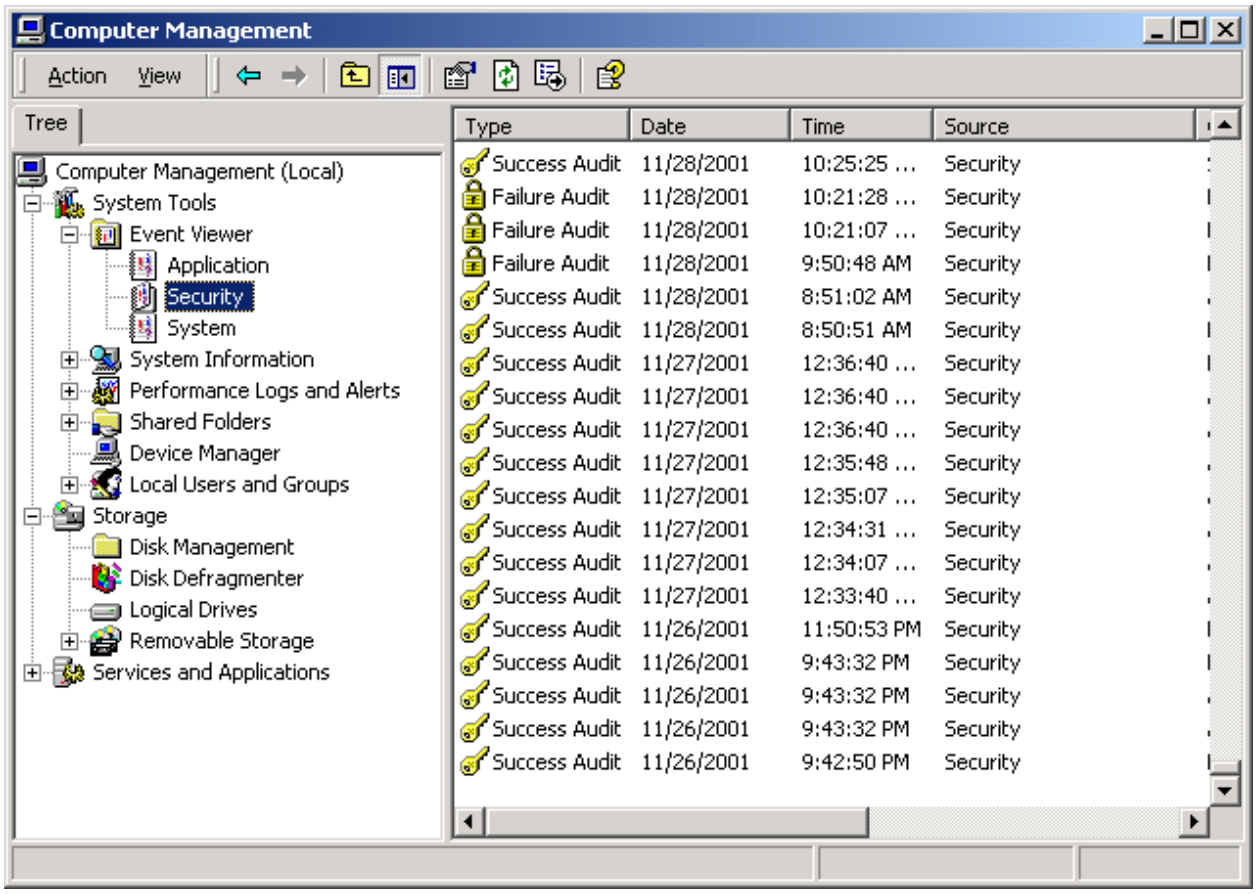

Figure 5-1. Event Viewer

5.1 Systemwide Auditing

Windows 2000 Professional provides a method to manually configure system-auditing settings through the use of the **Local Security Policy** node located in **Start | Settings | Control Panel | Administrative Tools | Local Security Policy**. The NIST recommended settings can be applied with the **Security Configuration and Analysis** snap-in or the **secedit.exe** tool by using the templates provided in Appendix B. To perform manual auditing configuration, open the **Local Security Policy** node; then, open the **Audit Policy** settings shown in Figure 5-2.

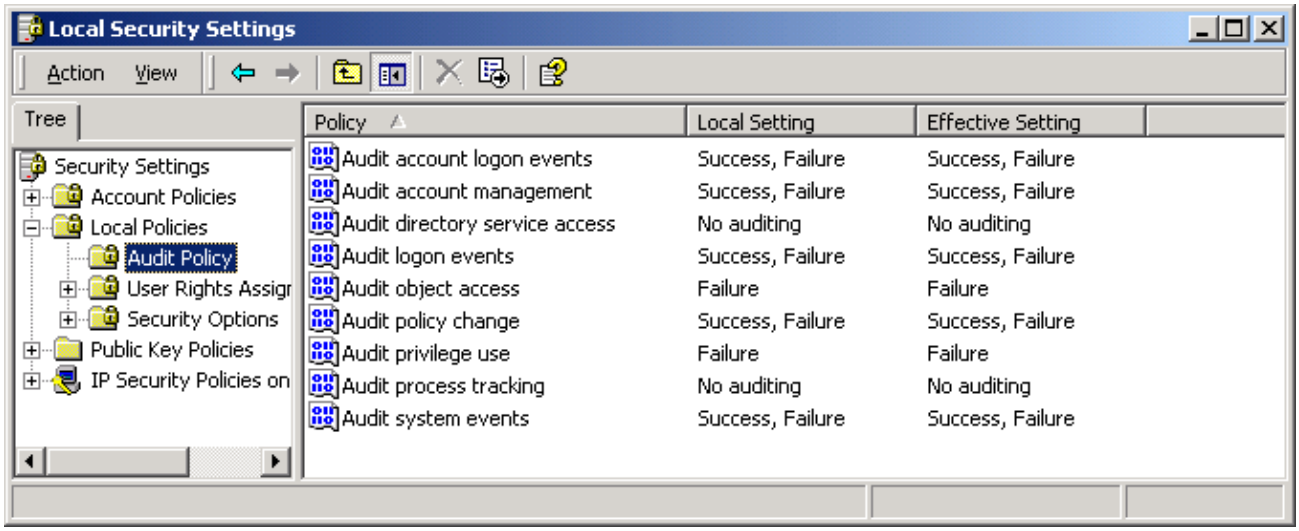

Figure 5-2. System-Wide Audit Policy

The policy areas are described in Table 5-1.

Table 5-1. Systemwide Audit Policy Description

Audit Policy	Description
Audit account logon events	Audits when a user logs on or off a remote computer from this workstation.
Audit account management	Audits when a user account or group is created, changed, or deleted; a user account is renamed, disabled, or enabled; a password is set or changed.
Audit directory service access	Audits the event of a user accessing an active directory object that has its own System Access Control List (SACL) specified.
Audit logon events	Audits users logging on, logging off, or making a network connection to the local computer.
Audit object access	Audits a user accessing an object (for example, a file, folder, registry key, or printer) that has its own SACL specified. **Note:** Auditing of success or failure of systemwide object access will create numerous log entries. Certain object access failures may be normal due to applications requesting all access types to objects, even though the application does not require all access types to function properly. Use object access auditing with caution.
Audit policy change	Audits every change to user rights assignment policies, audit policies, or trust policies.
Audit privilege use	Audits each instance of a user exercising a user right.
Audit process tracking	Audits detailed tracking information for events such as program activation, process exit, handle duplication, and indirect object access.
Audit system events	Audits when a user restarts or shuts down the computer or when an event occurs that affects either the system security or the security log.

5.2 Individual File Auditing

Windows 2000 Professional provides a method to monitor access to any file stored on its NTFS. This auditing method is typically used to monitor access to sensitive files. Individual file auditing is configured by right-clicking on the file, and then selecting **Properties**. Select the **Security** tab; then, click on **Advanced** as shown in Figure 5-3.

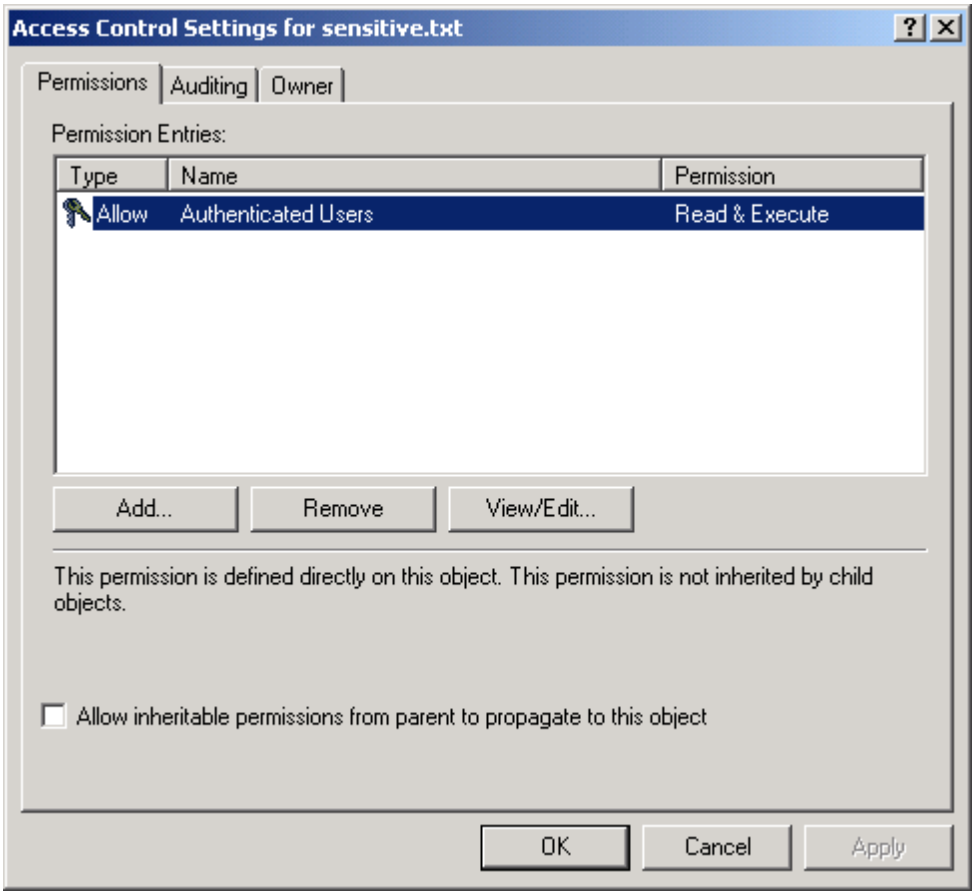

Figure 5-3. Advanced File Settings

Select the **Auditing** tab and **Add** a user as shown in Figure 5-4. Select what file permissions access attribute you wish to audit by clicking in the **successful** or **failed** checkboxes or none at all. The output of the system auditing can be viewed using the event viewer. The event viewer can be accessed using the **Computer Management** container located in the **Administrative Tools** folder.

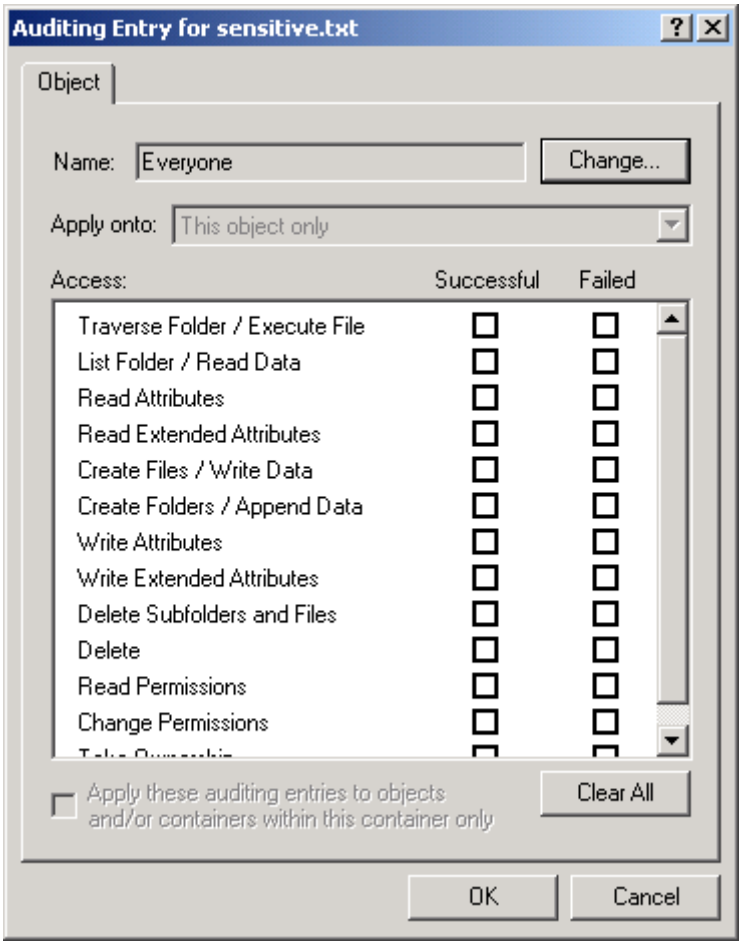

Figure 5-4. File Auditing

5.3 Summary of Recommendations

- Apply the NIST template to configure the auditing and event log policies. Refer to Appendix B for specific recommended values.
- Audit critical and sensitive personal data files.
- In low-risk environments, use the **Event Viewer** weekly to review the log files; in higher risk environments, review the log files daily.

6. Windows 2000 Professional Installation

The tools and configurations provided within this document were built and tested from a clean Windows 2000 Professional installation. It is recommended that SAs build their system from a clean formatted state to begin the process of securing Windows 2000 Professional workstation. It is also recommended that the installation process be performed on a secure network segment or off the network until the security configuration is completed and all patches are applied. In addition it is recommended that strong passwords be set for any accounts built in or created during the installation.

It is assumed that the readers have had some basic experience installing Windows products; therefore, the common installation steps for Windows 2000 Professional installs will not be discussed. If further information about these steps is required, refer to Microsoft's Windows 2000 installation guide. Key requirements to creating a secure system will be discussed in the sections below.

Note: Install only the minimum required services and networking components for your installation environment. NIST recommends that only **Microsoft Client Networking** and **Internet Protocol (TCP/IP)** networking services be installed. The NIST recommendations for removing unnecessary services are presented in Section 8.5.

6.1 Why Choose NTFS?

The initial step in creating a "clean" install of a Windows 2000 Professional system is choosing the file system for the hard drive. It is recommended that NTFS 5 be chosen over the file allocation table (FAT) file system and that the hard drive be formatted into two partitions for system and data areas. The system partition should contain the OS and applications; the data partition includes the user home directories.

Note: To change the location of the **My Documents** folder, **right-click My Documents | select Properties | enter the new location | click OK | allow movement of files within the original folder**.

Windows 2000 introduced a new version of NTFS, called NTFS 5, which provides additional security features to the Windows file system. Windows NT 4.0 uses the older version of NTFS; therefore, within a mixed NT/Windows 2000 environment, any Windows NT 4.0 machine that wishes to see network shares on a Windows 2000 Professional NTFS 5 partition must have installed Service Pack 4 or later. For the remainder of this document, NTFS 5 will be referred to as NTFS.

NTFS uses a file called the Master File Table (MFT) instead of the more common (FAT) to track all files and directories stored on a volume. This MFT contains a record for each resource stored on the physical disk, which includes information about the file to which it points, such as the owner, creation dates, file name, and a security descriptor.

The primary advantage of NTFS over alternate file systems is that each formatted byte on an NTFS partition contains bits reserved for discretionary access control (DAC) mechanisms like the access control list (ACL), discussed in greater detail in Section 8.1. Users should format the OS partition as NTFS because default file security and file auditing cannot be applied to a file system other than NTFS.

6.2 How to Convert Non-NTFS Partitions

Although it is strongly recommended that Windows 2000 Professional be installed on NTFS partitions, a functional reason may exist that causes a machine to keep its non-NTFS partitions. Non-NTFS partitions can be converted to NTFS at any time after the installation of Windows 2000 Professional using the

convert.exe utility. This utility, which is located within the **%SystemRoot%\system32**[1] directory, must be executed from an account with administrative privileges. The following sequence of steps will convert any Windows partition to NTFS:

- Open a command prompt.
  - Select **Run** from the **Start** menu, and type **cmd.exe** to open the Windows 2000 command interpreter.
- Type the following syntax on the command line: **C:\>convert <volume> /FS:NTFS [/V]**
  - Substitute the drive letter of the partition to convert for **<volume>**.
  - The **/V** switch is optional, which causes convert to run in verbose mode.
- Restart the system at completion.

  Note: This conversion will not occur immediately for **%SystemDrive%**[2] because the virtual memory page file could be in use simultaneously. In this case, when the system is rebooted, the conversion will occur.

  Note: After the conversion, the partition that has been converted has no file permissions set. To bring the converted system to a known security state, apply the **basicwk.inf** and the **ocfiles.inf** file from Microsoft using **secedit.exe** (see Section 2.2) before the NIST Windows 2000 Professional security template is applied. The inf files still leave some files and folders without security settings.
  NIST highly recommends that users start with a clean install of the NTFS file system and do not rely on the conversion utility.

6.3 Other settings

Enable a password-protected screen saver with a maximum wait time of 15 minutes. Rename the **Administrator** and **Guest** account; this can also be configured in the NIST template under **Local Policies | Security Options**. Enter the system BIOS and set a password to prevent unauthorized access to the system BIOS settings. In highly secure environments, the user may want to disable booting from devices other than the hard drive; many BIOS configurations allow the disabling of CD-ROM and floppy disk booting. Disable CD-ROM auto run; this setting is configured by the NIST template. Configure **Folder Options Views** with the following attributes: **show hidden files and folders and show extensions for known file types**. Consider mapping the **My Documents** folder to the data drive root directory. Disable the **Guest** account; this is configured by default within the NIST template. In addition, assign a strong 15-character password to the built-in **Guest** account.

6.4 Creating and Protecting the ERD

The Emergency Repair Disk is a group of files containing information designed to allow a user to recover from certain types of mishaps when using Windows 2000 Professional. The creation of an ERD is an extremely important step in the installation of a Windows 2000 Professional system. An ERD can repair and restore Partition Boot Sectors, system files, and environment files. It is recommended that the ERD

[1] %SystemRoot% refers to the WINNT directory located on the system drive (i.e. C:\).
[2] %SystemDrive% refers to the C:\ drive that contains the system directory.

be created after the system is securely configured. This is not, however, the only step that should be taken.

The ERD contains sensitive information about Windows 2000, including password information that can be used to subvert the security measures and gain privileged access. This information must be protected. The following sections address the recommended methods creating the ERD and the methods of protecting the sensitive data it contains

6.4.1 How to Create an ERD

To create an ERD on Windows 2000 Professional, log into an administrative privileged account and open the Backup and Recovery Tools window. To open this window, click sequentially the following series of menu commands:
Start | Programs | Accessories | System Tools | Backup
this action will open the **Backup and Recovery Tools** program window, as shown in Figure 6-1.

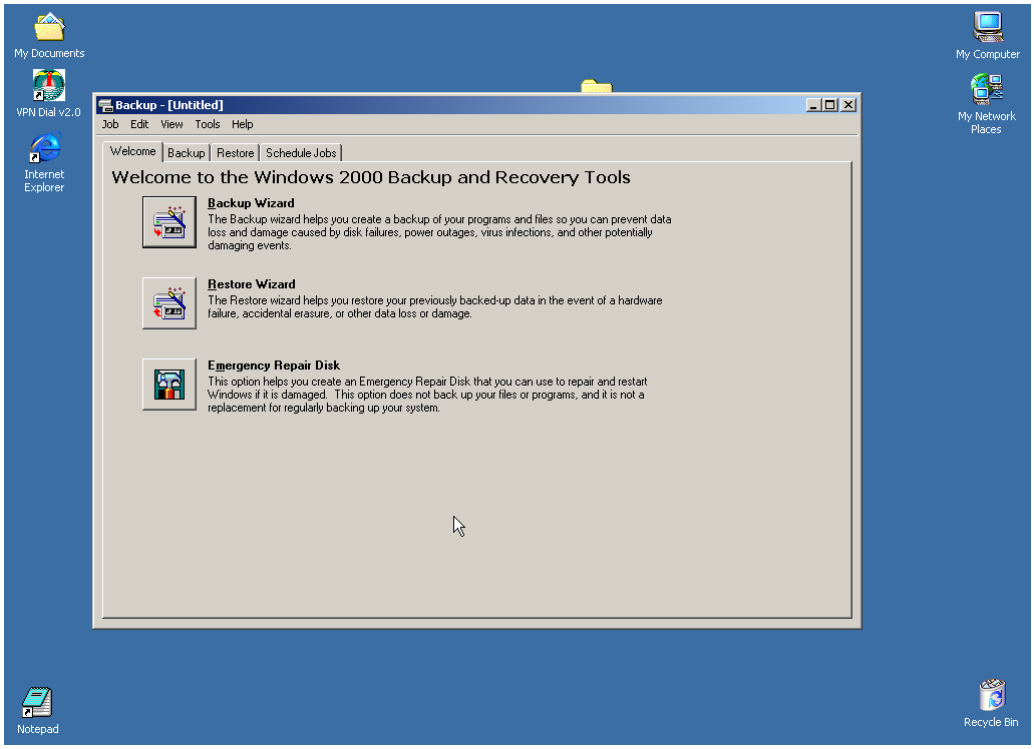

Figure 6-1. Open Windows 2000 Backup and Recovery Tools

From the Backup and Recovery Tools window, click the **Tools** tab and select **Create Emergency Repair Disk** from the menu bar; the subsequent steps are self-explanatory.

Note: As a matter of best practice, an ERD should ALWAYS be re-created when any configuration change is made to Windows 2000 Professional.

6.4.2 How to Protect ERD

Because the ERD is necessary for repairing vital parts of the Windows 2000 Professional OS, it contains information that must be protected to ensure system integrity. When an ERD is created, a copy of the

SAM database is copied to the location where the ERD is stored. This file contains usernames and password hashes that can be imported into a password-cracking program. If a malicious user obtains a copy of a SAM file from a Windows 2000 Professional machine, the user will be able to brute-force crack the encrypted passwords. The removable media used to store the ERD should be labeled sensitive and stored in some type of locked storage area (e.g., a filing cabinet, fireproof lockbox, or supply room).

6.4.3 How to Protect ERD Backup

By default, a backup ERD is stored in the **winnt\repair** directory on the Windows 2000 Professional system partition. An additional SAM file is included in the contents of the backup ERD, as shown in Figure 6-2**.**

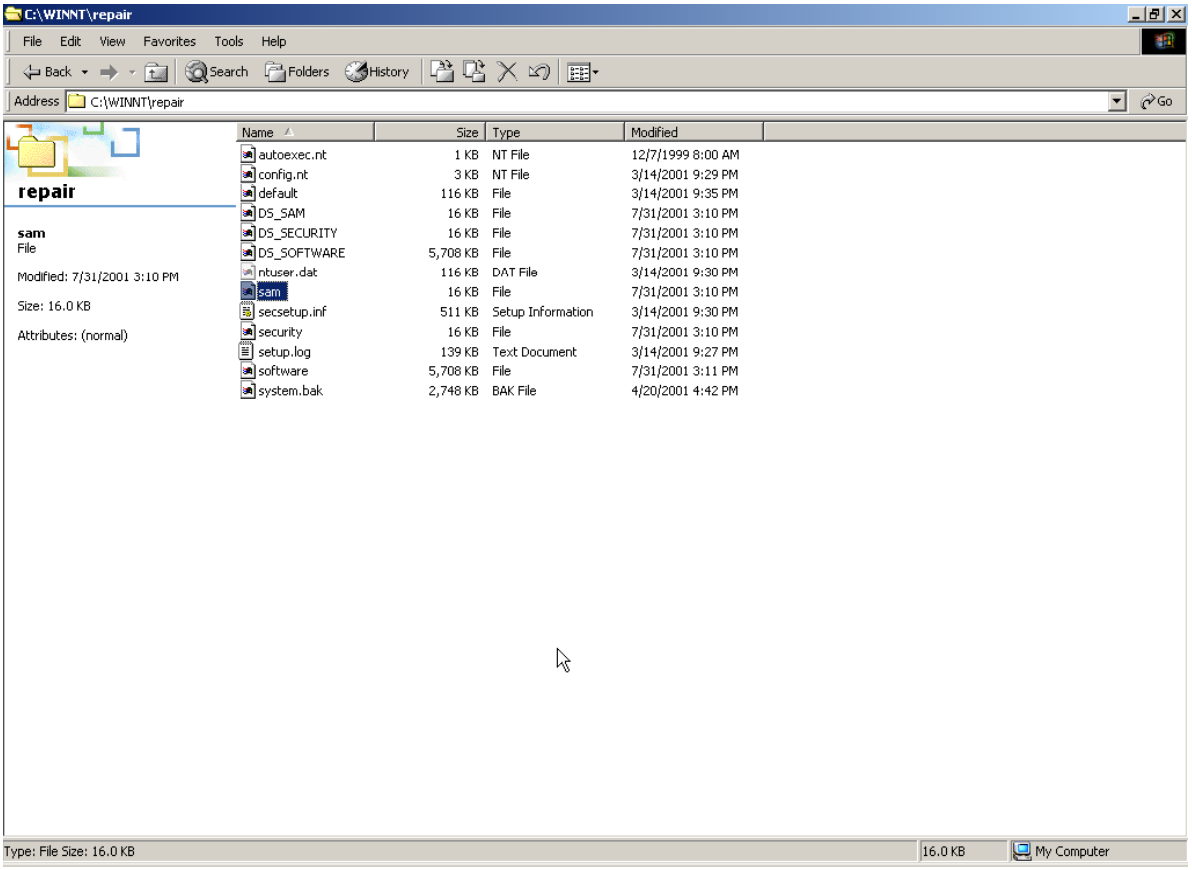

Figure 6-2. Backup ERD Showing SAM File

It is recommended that the files within the repair directory be deleted after a copy on removable media is securely stored away. Access to the repair directory should also be restricted; the recommended method for restricting access to the **winnt\repair** directory is to delete it or to set the NTFS permissions to include administrative-level users ONLY, as shown in Figure 6-3. If it is determined that any user account or group has unnecessary access to this folder, access can be removed by highlighting that entry and clicking the **Remove** button.

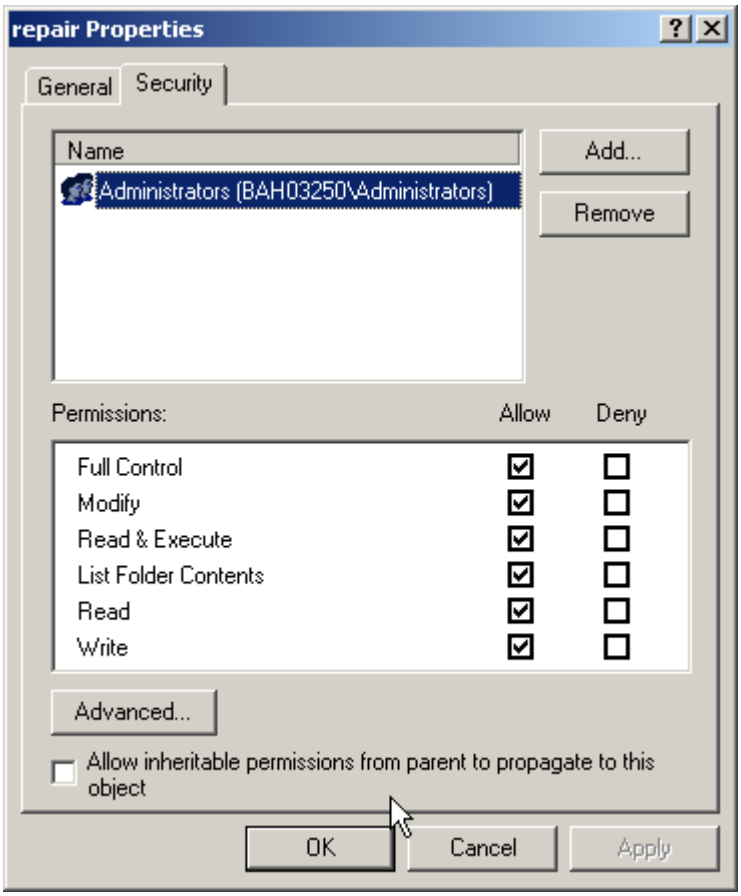

Figure 6-3. Restrict NTFS Permissions for winnt\repair Directory

6.5 Summary of Recommendations

- Partition the hard drive using NTFS for system and data files.
- Install OS with minimum required services.
- Install **Internet Protocol (TCP/IP)** networking and **Client for Microsoft Networking** only.
- Secure the **winnt\repair** directory. The NIST security template completes this action automatically.
- Create the ERD when security configuration is complete.
- Securely store the ERD on removable media.
- Delete or restrict access to the backup ERD from the **winnt\repair** directory.

This page intentionally left blank

7. Updating and Patching Guidelines

Windows 2000 Professional users have two main methods to update Windows systems: service packs or hotfixes. The Windows service pack provides improvements and replacements to OS components. Security updates and hotfixes usually address some vulnerability that was discovered in common components of Windows or additional Microsoft applications. The following sections discuss the various methods of obtaining and applying patches and updates to Windows 2000 Professional.

For further information about System Updating and Patching, refer to **NIST Special Publication 800-40 Applying Security Patches**, available at http://csrc.nist.gov/publications/nistpubs/

7.1 Windows 2000 Professional Updates

Microsoft publishes updates to the Windows OS in the form of service packs and hotfixes. The service packs and hotfixes can be obtained in two ways: downloading from the Internet and ordering a CD containing the files. Microsoft Service Pack (SP3), the latest service pack, may be downloaded from the following Uniform Resource Locations (URL):
http://www.microsoft.com/windows2000/downloads/servicepacks/sp3/default.asp

Note: Always perform a backup of any critical files and create an ERD before performing any patching. Fully test the patches on nonoperational systems before deploying.

Note: Do not attempt any service pack installation unless you have sufficient hard drive space! This action could cause extensive file system damage.

Note: Service Pack 3 installs the Automatic Update client that can be used to keep the system current automatically by installing the critical updates, most of which are security related. Two new services are added to the system. Automatic Updates service run automatically and Background Intelligent Transfer Service is configured to execute manually when the system starts. The Automatic Updates found in the control panel can be used to modify the settings. Refer to the local policy to determine it is appropriate to enable or disable the automatic update. To disable Automatic Updates, configure the system not to keep the computer up to date in the control panel and disable the Automatic Updates and Background Intelligent Transfer services. These services are not defined in the NIST security templates.

Note: Microsoft provides a command line tool to automate the process of determining the hotfixes required for your computer. This tool, called **hfnetchk.exe,** is located at http://support.microsoft.com/default.aspx?scid=kb;EN-US;q303215. The tool can be used to check locally and remotely the status of patching on a Windows 2000 system.

Note: Multiple hotfixes can be applied in a batch file without rebooting between installations by using the Microsoft command-line **QChain.exe** tool. The tool is located at http://support.microsoft.com/default.aspx?scid=kb;EN-US;q296861.

Note: qfecheck.exe is a Microsoft command line tool that can be used to track and verify installed hotfixes. The tool can be downloaded from http://support.microsoft.com/default.aspx?scid=kb;en-us;Q282784.

Table 7-1 lists the Security Bulletins included in SP3 (August 2002) for Windows 2000 Professional.

Table 7-1. Security Bulletins Included in Service Pack 3

MS00-077 (Q299796) – Patch Available for "NetMeeting Desktop Sharing" Vulnerability
MS00-079 (Q276471) – Patch Available for "HyperTerminal Buffer Overflow" Vulnerability
MS01-004 (Q285985) – Malformed .HTR Request Allows Reading of File Fragments
MS01-007 (Q285851) – Network DDE Agent Requests Can Enable Code to Run in System Context
MS01-011 (Q287397) – Malformed Request to Domain Controller Can Cause CPU Exhaustion *(superseded by MS01-024)*
MS01-013 (Q285156) – Windows 2000 Event Viewer Contains Unchecked Buffer
MS01-022 (Q296441) – WebDAV Service Provider Can Allow Scripts to Levy Requests as User
MS01-024 (Q294391) – Malformed Request to Domain Controller Can Cause Memory Exhaustion
MS01-025 (Q296185) – Index Server Search Function Contains Unchecked Buffer
MS01-026 (Q293826) – May 14, 2001, Cumulative Patch for IIS
MS01-031 (Q299553) – Predictable Named Pipes Could Enable Privilege Elevation via Telnet
MS01-033 (Q300972) – Unchecked Buffer in Index Server ISAPI Extension Could Enable Web Server Compromise
MS01-035 (Q300477) – FrontPage Server Extension Sub-Component Contains Unchecked Buffer
MS01-036 (Q299687) – Function Exposed via LDAP over SSL Could Enable Passwords to be Changed
MS01-037 (Q302755) – Authentication Error in SMTP Service Could Allow Mail Relaying
MS01-040 (Q292435) – Invalid RDP Data Can Cause Memory Leak in Terminal Services
MS01-041 (Q298012) – Malformed RPC Request Can Cause Service Failure
MS01-042 (Q304404) – Windows Media Player .NSC Processor Contains Unchecked Buffer
MS01-043 (Q303984) – NNTP Service in Windows NT 4.0 and Windows 2000 Contains Memory Leak
MS01-044 (Q301625) – 15 August 2001 Cumulative Patch for IIS
MS01-046 (Q252795) – Access Violation in Windows 2000 IRDA Driver Can Cause System to Restart
MS01-052 (Q307454) – Invalid RDP Data Can Cause Terminal Service Failure
MS01-060 (Q305601) – SQL Server Text Formatting Functions Contain Unchecked Buffers
MS02-001 (Q311401) – Trusting Domains Do Not Verify Domain Membership of SIDs in Authorization Data
MS02-004 (Q307298) – Unchecked Buffer in Telnet Server Could Lead to Arbitrary Code Execution
MS02-006 (Q314147) – Unchecked Buffer in SNMP Service Could Enable Arbitrary Code to be Run
MS02-011 (Q313450) – Authentication Flaw Could Allow Unauthorized Users To Authenticate To SMTP Service
MS02-012 (Q313450) – Malformed Data Transfer Request Can Cause Windows SMTP Service to Fail
MS02-013 (Q300845) – 04 March 2002 Cumulative VM Update
MS02-014 (Q313829) – Unchecked Buffer in Windows Shell Could Lead to Code Execution
MS02-016 (Q318593) – Opening Group Policy Files for Exclusive Read Blocks Policy Application

MS02-017 (Q311967) – Unchecked Buffer in the Multiple UNC Provider Could Enable Code Execution

MS02-018 (Q319733) – Cumulative Patch for Internet Information Service

MS02-024 (Q320206) – Authentication Flaw in Windows Debugger Can Lead to Elevated Privileges

MS02-028 (Q321599) – Heap Overrun in HTR Chunked Encoding Could Enable Web Server Compromise

MS02-029 (Q318138) – Unchecked Buffer in Remote Access Service Phonebook Could Lead to Code Execution

Internet Explorer 5.5 and Internet Explorer 6 security patches are NOT included in Windows 2000 Service Pack 3. Customers running Internet Explorer 5.5 are encouraged to review and apply security patches (related to their IE 5.5 Service Pack) identified here:
http://www.microsoft.com/technet/security/current.asp?productID=80&servicePackId=0

Customers running Internet Explorer 6 are encouraged to review and apply security patches (related to their IE 6.0 Service Pack) identified here:

http://www.microsoft.com/technet/security/current.asp?productID=119&servicePackId=0

Security patches for issues affecting Internet Explorer 5.01 Service Pack 2 have been included in Windows 2000 Service Pack 3. Specifically, IE 5.01 Service Pack 2 patches referenced in the following security bulletins are included in Windows 2000 Service Pack 3:

MS01-051(Q306121) – Malformed Dotless IP Address Can Cause a Web Page to Be Handled in the Intranet Zone

MS01-055 (Q312461) – Internet Explorer Cookie Data Can Be Exposed or Altered Through Script Injection

MS01-058 (Q313675) – File Vulnerability Patch for Internet Explorer 5.5 and Internet Explorer 6

MS02-005(Q316059) – February 11, 2002, Cumulative Patch for Internet Explorer

During the service pack installation process, the user is presented with an option to back up the service pack files being installed to allow the possibility of uninstalling them at a later date. Each administrator must make this choice. If the decision is to retain the ability to revert to a prior service pack, then the directory containing the prior service packs or hotfix files **C:\winnt\$[folder name]$** must be secured by setting the NTFS permissions to include SAs only.

7.2 Windows 2000 Patching Resources

Microsoft has developed numerous ways of distributing fixes and patches for vulnerabilities discovered in the Windows 2000 OS. Microsoft's own security site and third party organizations, commonly referred to as security portals, serve as excellent methods of notification upon discovery and publication of a new Windows vulnerability.

Note: System patching should be performed in accordance with established procedures within your organization.

7.2.1 Internet Security Portals

Table 7-2 shows a partial listing of Internet locations of security portals that track Microsoft Windows vulnerabilities beginning with Microsoft's own security portal. This list is incomplete and does not suggest any type of commercial endorsement.

Many of the Web sites listed offer mailing lists as a means to alert subscribed users of the publication to a new vulnerability. It is recommended that users and administrators of Microsoft Windows 2000 Professional subscribe to one or more of these lists, in particular the Microsoft Security Mailing list. This is a proactive means of staying on top of the latest events affecting Windows security. Consult the specific Web sites for instructions regarding how to subscribe to each list.

Table 7-2. Information Security Portals

Name	URL
Microsoft	http://www.microsoft.com/technet/security
ICAT	http://icat.nist.gov/
CERT	http://www.cert.org/
Security Focus	http://www.securityfocus.com/
NT Bugtraq	http://ntbugtraq.ntadvice.com/
Xforce	http://xforce.iss.net

7.2.2 Windows Update Web Site

Microsoft has provided consumers with an automated site to distribute patches located at the following URL: http://windowsupdate.microsoft.com

Microsoft also provides a patching site targeted at business users called Windows Update Corporate. Microsoft makes many of the security updates available to allow users and SAs to download patches for distribution. This site is located at http://www.microsoft.com/windows2000/downloads/default.asp.

Windows Update has ActiveX Controls and active scripting to display content correctly and to determine which updates apply to the inspected system. Users can automatically link to the Microsoft Windows Update Web site from the **Tools** menu on **Internet Explorer**. Figure 7-1 shows an example of the Windows Update Web site. It is recommended that the user install the critical and security updates package.

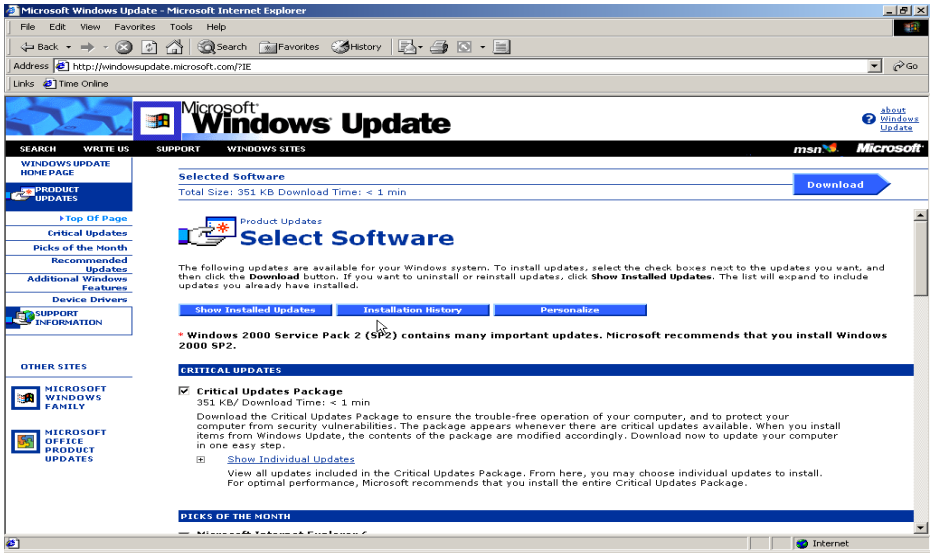

Figure 7-1. Windows Update Web Site

Microsoft has taken steps to automate this process by using the Windows Update Critical Notification software. This piece of software, which can be downloaded from the Windows Update Web site automatically, checks back with the Web site to determine if any critical updates need to be installed. If it finds such updates, the software displays an alert on-screen notifying the user of the situation. Ensure that the automatic updating of installed software conforms to local policy before enabling this feature.

7.3 Summary of Recommendations

- Subscribe to the Microsoft Security mailing list and others.
- Periodically scan systems to determine patch status using Windows Update Web site or the **hfnetchk.exe** tool.
- Use the Microsoft Security site as a portal to search and download security patches.
- Test and apply patches when required.
- Update or create a new ERD after the system has been patched.

This page intentionally left blank

8. Windows 2000 Pro Configuration Guidelines

This section addresses the necessary security configuration guidelines for Windows 2000 Professional based on the type of machine created. The two types of machine configurations addressed in this section are a stand-alone machine connected to a network and a Windows 2000 domain member. Regardless of the type of machine created, the roles that the machine will play should be limited.

It is important to consider the concept of security for a Window 2000 Professional workstation as an ongoing task. The recommendations presented in this section do not entail the complete set of possible security considerations and concerns for the entire life cycle of a Windows 2000 Professional workstation. Systems administrators and end users should consider every decision made regarding their workstations and what effect that decision might have on its security.

8.1 Securing the File System Using ACLs

All partitions created during installation of Windows 2000 Professional should be formatted with NTFS. Upon completion of the physical installation of Windows 2000 Professional, additional steps should be taken concerning the file system access control mechanisms that are not included in the installation process. These important steps are outlined in this section. (The EFS is discussed in detail in Section 8.2.) This section also addresses additional steps that can be taken to enhance the security of the file system.

The following standard notation is used to discuss the Windows 2000 file system and partitions:

%SystemDrive% – refers to the actual partition or hard drive in which Windows 2000 Professional is installed, usually the **C:** drive.

%SystemRoot% – refers to the folder on **%SystemDrive%** where Windows 2000 Professional files are installed, usually the **WINNT** directory.

8.1.1 File System ACL

General instructions regarding the configuration and setting of file system access control entries (ACE) and ACLs for Windows 2000 Professional are included in this section. All recommended ACL and ACE settings will be set by the use of the NIST security templates included in Appendix B. Additional settings will be specific to the environment in which the Windows 2000 Professional machine resides. The following section provides general information about customizing settings for an environment.

8.1.2 Setting ACLs

Changes to a resource ACL can be made using one of three possible methods. The first method is to open the properties window for a resource from its context menu. The second method is to use the utility **cacls.exe** found in **%SystemRoot%\system32**. This is a command line interface used to set file ACLs, but it does not set Windows 2000 security descriptors. The third method is the use of the **MMC Security Template** snap-in and one of the provided security templates in Appendix B to apply its recommended settings.

8.1.3 ACL Example

On a Windows 2000 partition, users can set ACLs for specific resources, be it a file or folder, by opening the **Properties** window from that resource's context menu and clicking on the **Security** tab. Figure 8-1

shows a sample ACL. For consistency, each entry that binds a security identifier (SID) to a set of permissions within an ACL is referred to as an ACE.

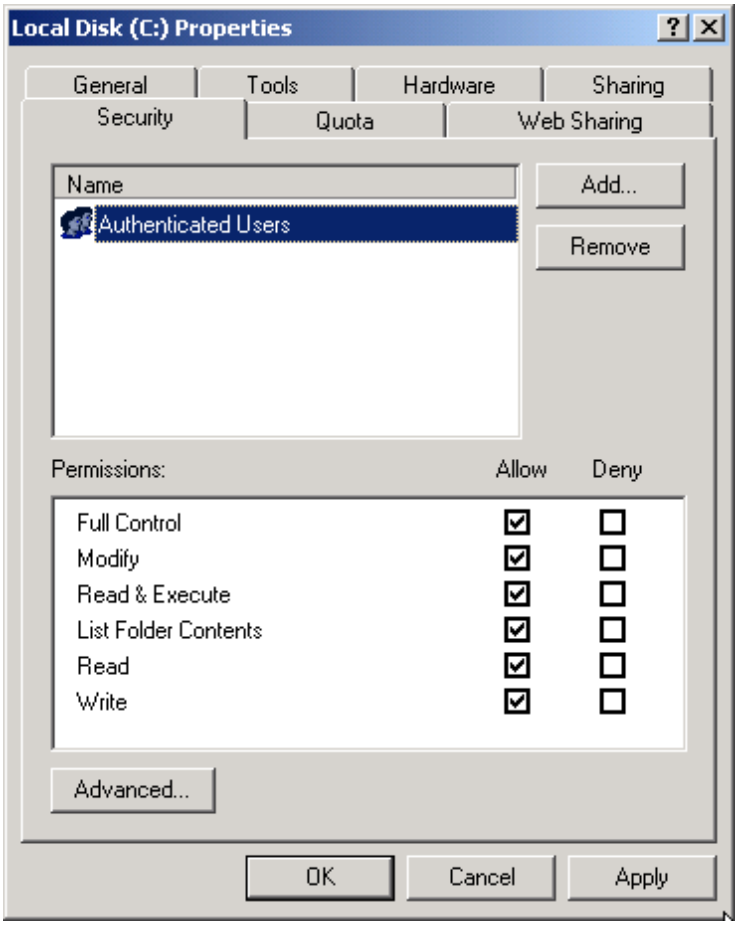

Figure 8-1. ACL for Sample System Partition

8.1.4 Windows 2000 Access Control

Windows 2000 uses an inheritance model for assigning ACEs. An object's ACL can contain ACEs that it inherited from its parent container. For example, a file in an NTFS can inherit ACEs from the directory that contains it. Clicking on the advanced button, shown in Figure 8-1, illustrates Windows 2000 support of automatic propagation of an inheritable ACE. In addition, an ACE that is directly applied to a file system object is given a higher priority than an inherited ACE. The directly applied ACE overrides any conflicting inherited ACEs.

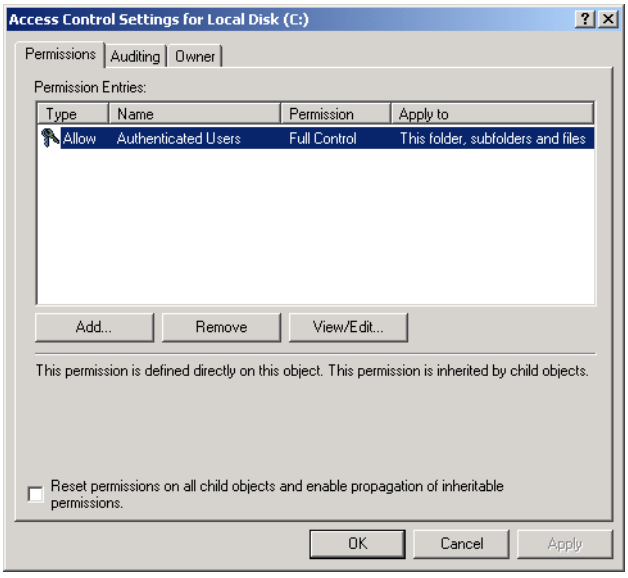

Figure 8-2. Advanced ACL Window for Sample System Partition, Access Control Settings Screen

In the example shown in Figure 8-2, the **Authenticated Users** group has **full control** over the entire **C:** partition. Clicking the **View/Edit** button displays finer detail of settings, allowing a user to decide with much more control what a user or group can do to a file, folder, subfolder, or combination of the three, as shown in Figure 8-3.

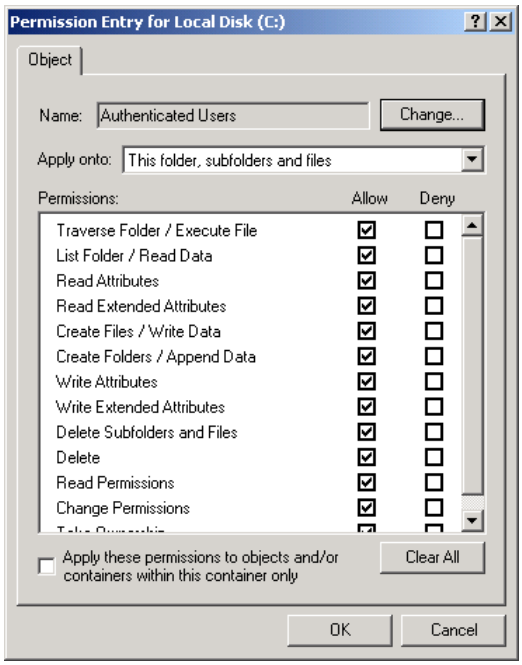

Figure 8-3. Advanced ACL window for sample system partition, Permission Entry Screen

8.1.5 Replace Default Access Rights

In a default Windows 2000 Professional installation, the **Everyone** group has full access to root partitions. It is recommended that the **Everyone** group be changed to the **Authenticated Users** group

wherever possible. This action will ensure that anonymous users and guests have no access to the resource. In some isolated cases, the **Everyone** group may not be replaced as a result of application requirements, **test your settings before deployment.**

Restrict access to administrative tools and utilities. Windows 2000 Professional provides many command line utilities to assist with the administration of the system. Access to these utilities is granted to all users by default. It is recommended that access to these utilities be restricted to **Administrative Users**. Examples of these utilities include **rpc.exe, regedt32.exe,** and **rexec.exe**.

8.2 Encrypted File System

EFS is designed to address numerous concerns regarding the integrity of data stored on secondary storage within Windows 2000. EFS is designed to keep data private and unreadable to unauthorized users. With physical access, malicious users can boot a computer system into a file system other than NTFS effectively bypassing all security provided by NTFS, thus gaining access to all unencrypted files residing on the hard drive. EFS was designed to reduce the risks associated with mobile computing and unauthorized physical access through file encryption.

8.2.1 How Does EFS Work?

EFS underlying technology was presented briefly in Section 2.6. The EFS, which is based on public-key encryption, integrates tightly with the PKI features that have been incorporated into Windows 2000 Professional. The actual logic that performs the encryption is a system service that cannot be shut down. This program feature is designed to prevent unauthorized access, but has an added benefit of rendering the encryption process completely transparent to the user. Each file that a user may encrypt is encrypted using a randomly generated file encryption key (FEK).

8.2.2 How Is EFS Implemented?

It is recommended that an encryption folder be created for sensitive files. Once a folder is set to encrypt its contents, the user is given the choice to apply this change to every resource within the folder or to apply the attributes only to the current folder. The dialog box confirming this attribute change is shown in Figure 8-4.

Figure 8-4. Confirm Application of EFS Encryption to Current Resource

EFS is implemented in one of three possible ways: from the properties window of a folder, within the **My Computer** window, and from the **Windows Explorer**.

8.2.3 EFS Example

This sample process describes how to implement EFS for a sample folder from within the **My Computer** window. The default configuration of EFS allows a user to encrypt and decrypt files immediately without any administrator interaction. Figure 8-5 shows the directory listing from the **My Computer** window for **Sample Folder**. Note that its only contents are the text file **Sample.txt** created by the **WordPad** utility.

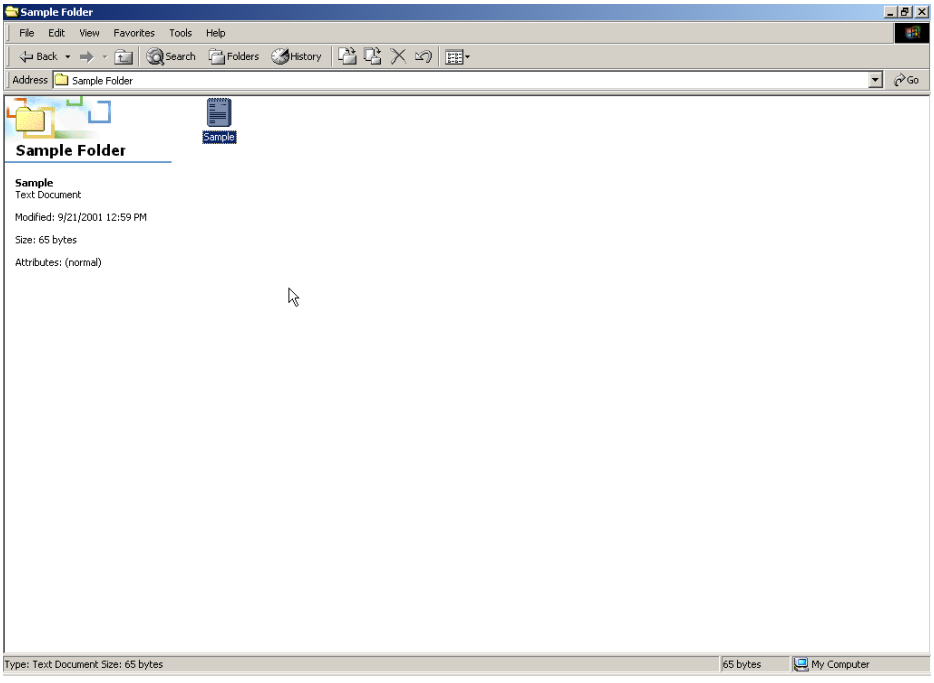

Figure 8-5. Directory Listing with Sample Folder

In this example, the folder attributes on the left side of the window clearly show that the highlighted text file Sample.txt is not encrypted. Although the file **Sample.txt** may be encrypted itself, it is recommended

that encryption be enabled by opening the **Advanced Properties** window of the folder from one level higher in the directory tree, which frees the user from worrying about individual files. Figure 8-6 shows the **Advanced Properties** window for the folder **Sample Folder**, where encryption is enabled.

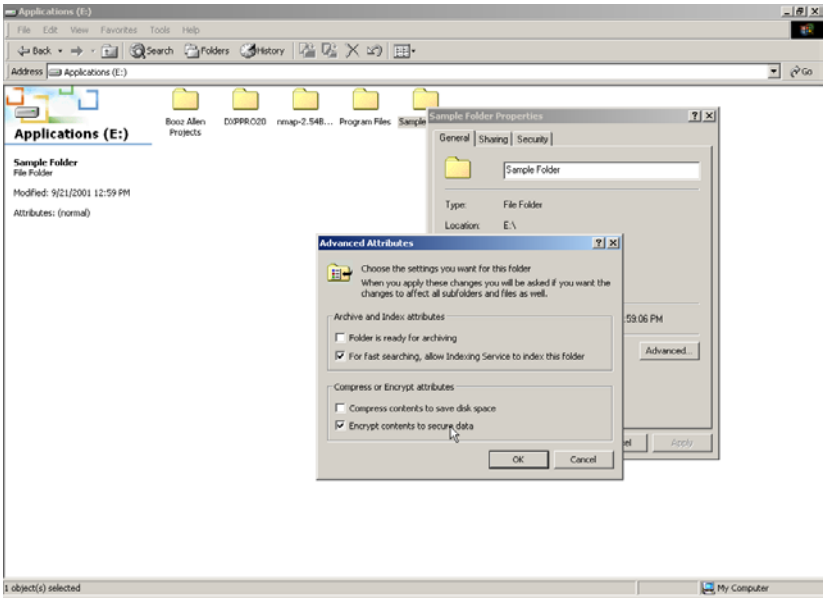

Figure 8-6. Advanced Attributes Window for Sample Folder

Once the checkbox **Encrypt contents to secure data** is checked and the window is closed, the attributes for the file **Sample.txt** within the **Sample Folder** should change to reflect this change in folder attributes. Confirm this change by pressing the **OK** button. Figure 8-7 shows the updated directory listing for **Sample Folder**. Note that the attributes of **Sample.txt** now reflect the newly encrypted status.

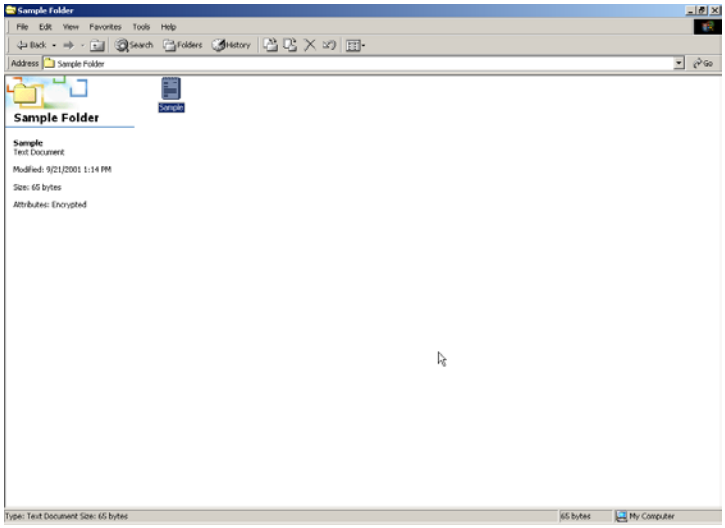

Figure 8-7. Updated Directory Listing of Sample Folder

Although the initial release of EFS did not support file sharing, this functionality was included in the Service Pack 1 update for Windows 2000.

Note: EFS will successfully encrypt files on network shares, yet the data will not be encrypted while in transit. To protect data in transit, a technology such as secure socket layer (SSL) or IPsec should be implemented.

Note: Files are automatically decrypted when they are moved into a folder not designated as **Encrypt contents to secure data.**

As stated previously, this process is transparent to the end user because EFS is integrated with NTFS. If an alternate user of similar or lesser privileges were to attempt to open this file, because the user does not have the FEK, the user would be unable to access it. In some cases, access restrictions such as these may require authorized users to implement data recovery procedures. If the owner of the folder or file were to have his or her key-pair corrupted, the file would be rendered inaccessible without a recovery agent. It is recommended that the recovery agent be changed from the default Administrator account to a newly created EFS recovery agent account in a domain environment.

8.2.4 EFS Data Recovery

Windows 2000 EFS provides integrated data recovery support. The Windows 2000 security infrastructure enforces the configuration of data recovery keys so well that EFS is inaccessible unless one or more recovery keys are created. This is typically done during the installation process. By default, the recovery agent is the **Administrator**, as shown in Figure 8-8. EFS will allow recovery agents to configure public keys that are used to enable file recovery. Only the file's randomly generated encryption key is available using the recovery key, not a user's private key. This action ensures that no other private information is revealed accidentally to the recovery agent.

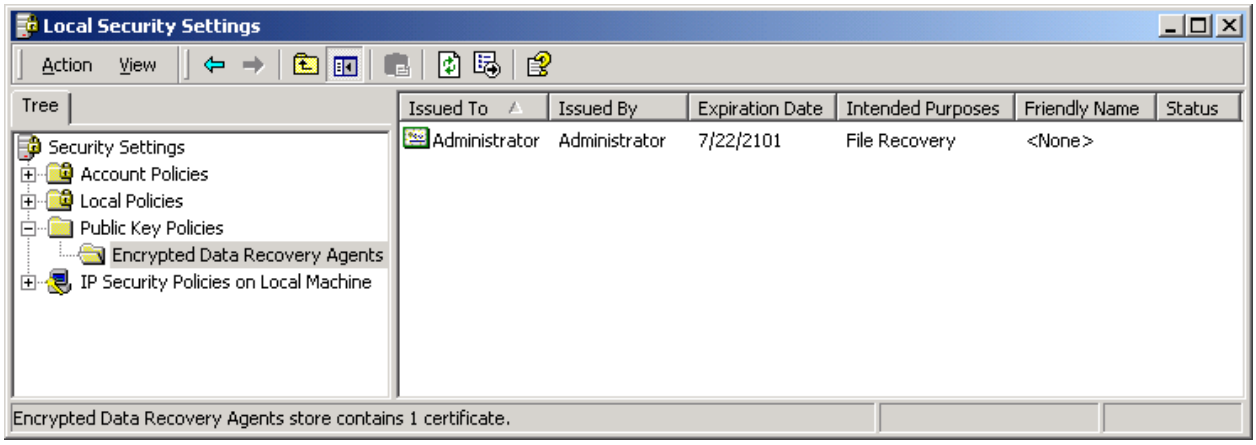

Figure 8-8. Recovery Agent Default Setting

The recovery keys contained in the **Encrypted Date Recovery Agents** folder can be backed up to removable media by logging into the system with the **Built-in Administrators** account and performing the following actions:

- Open the **Encrypted Data Recovery Agents** folder.
- Right-click the Certificate you would like to export.
- Choose **All Tasks | Export**.
- Save the file to removable media.

Note: For maximum security, the EFS recovery certificate can be removed from the computer after a successful backup by selecting the **Delete Private Key if the Export is Successful** checkbox.

8.3 Additional File System Security Measures

Additional steps can be taken to enhance the security of the file systems on Windows 2000 Professional that extend beyond ACLs and EFS. The Windows 2000 OS includes OS2 and Portable Operating System Interface for Computer Environment (POSIX) compliant environmental subsystems that allow Windows to run applications written for these operating systems. These resources should be removed unless they are necessary.

Windows 2000 data remnants allow images of resources to remain accessible after they should no longer be available. For example, Windows 2000 has an invisible directory called Recycler, which is used to maintain a copy of data marked for deletion until it is permanently removed from the Recycle Bin. In a default configuration, the Windows 2000 virtual memory page file is not wiped clean during any type of system shutdown. Under normal operation, the Virtual Memory Manager provides file protection for the page file. This section discusses how to remove unnecessary subsystems and protect against data remnants.

8.3.1 Removal of OS2 and POSIX

The Windows 2000 Professional architecture includes applications programming interfaces (API) to emulate the OS2 and any POSIX-compliant OS. These features allow applications written for these OSs to be run on a Windows 2000 Professional machine. Because these subsystems can introduce vulnerabilities into a Windows 2000 Professional machine, it is recommended that they be removed.

Removing the OS2 and POSIX subsystems is a two-step process: removing the subsystem executables and removing the subsystem registry keys. Windows 2000 Professional stores backup copies of all running system DLLs in the **%SystemRoot%\system32\dllcache** folder. Successful manual removal of system files requires removal from two locations. To remove all subsystem executables, delete the following files from **%SystemRoot%\dllcache** folder:

- **os2.exe**
- **os2ss.exe**
- **os2srv.exe**

Remove the following files from the **%SystemRoot%system32** directory:

- **os2.exe**
- **os2ss.exe**
- **os2srv.exe**
- **psxss.exe**
- **posix.exe**

Figure 8-9 shows the **%SystemRoot%** directory of a default Windows 2000 Professional installation. Note that the OS2 environment subsystem binaries have not been deleted.

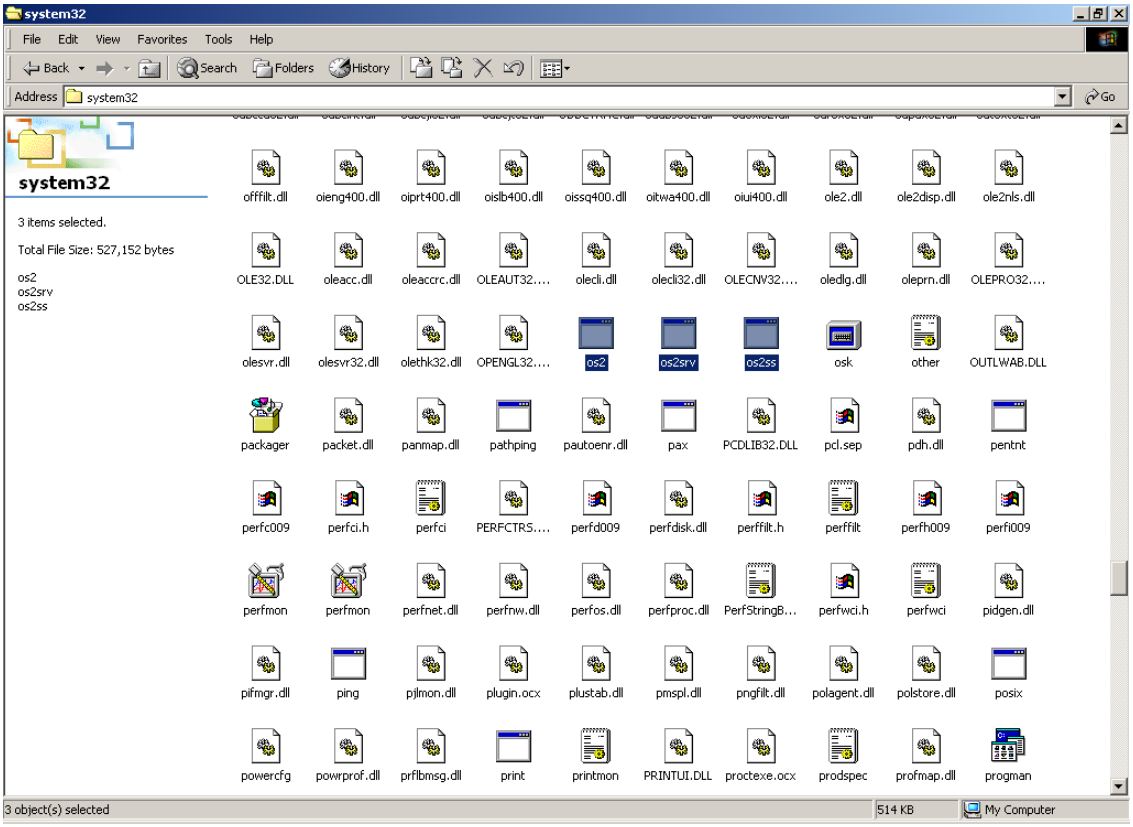

Figure 8-9. Updated Folder Listing of Sample Folder

To remove the subsystem registry entries, delete the following values from the **HKEY_LOCAL_MACHINE** hive:

- **\System\CurrentControlSet\Control\Session Manager\Environment\OS2LibPath**
- **\System\CurrentControlSet\Control\Session Manager\Subsystem\Optional**
- **\System\CurrentControlSet\Control\Session Manager\Subsystem\OS2**
- **\System\CurrentControlSet\Control\Session Manager\Subsystem\Posix**

These registry values contain information that pertains to locations and parameters for the OS2 and POSIX environmental subsystems. Once the subsystem binaries have been deleted, the values are no longer necessary.

8.3.2 Prevent Data Remnants

Data remnant is a concept where data remains accessible on a system even after it has been deleted. Memory dumps can include passwords and other sensitive information, and it is recommended that they be disabled. The recycle bin contains a hidden directory **RECYCLER** that stores a copy of recently deleted files. The virtual memory page file should also be wiped clean on each system shutdown for the same reasons. A number of options introduce data remnant threats in an out-of-the-box configuration of Windows 2000 Professional.

To disable memory dumps on Windows 2000 Professional, open the **System** applet on the **Control Panel**. Once the System applet window is displayed, click on the **Advanced** tab and click the **Startup and Recovery** button at the bottom. This action opens the Startup and Recovery properties window. Set the **Write Debugging Information** to **none** from the dropdown list, as shown in Figure 8-10.

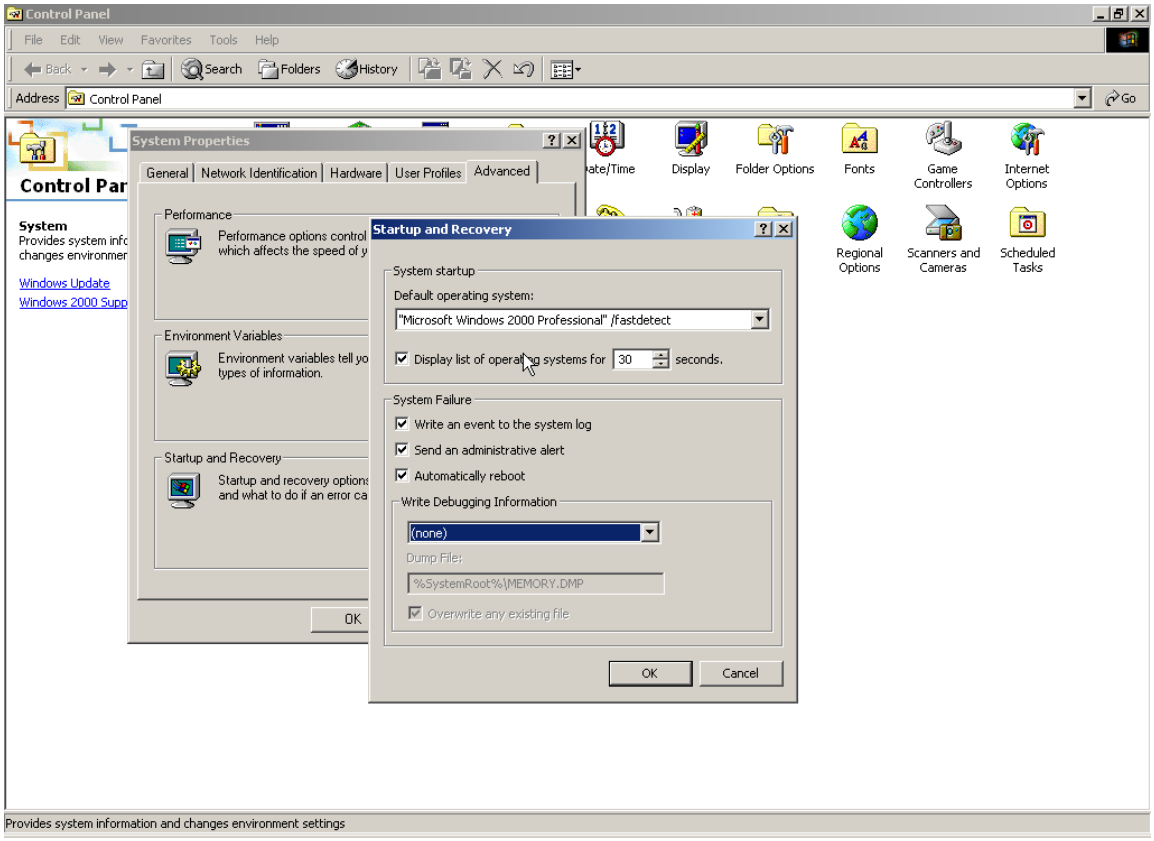

Figure 8-10. Disable Operating System Memory Dumps

> **Note:** The Windows 2000 OS is not the only source of memory dumps! Additional software such as Dr. Watson can create memory dumps if an application error occurs. It is recommended that users search their hard drives periodically to find and remove any file with an extension of **dmp**.

To set the Recycle Bin for immediate deletion of all files, open the recycle bin **Properties** window from its context menu by right-clicking on the **Recycle Bin** icon on the desktop. As in the example below, click on the checkbox that says **Do not move files to Recycle Bin. Remove files immediately when deleted**. This action prevents a copy of any future file that is deleted from being stored in the Recycle Bin.

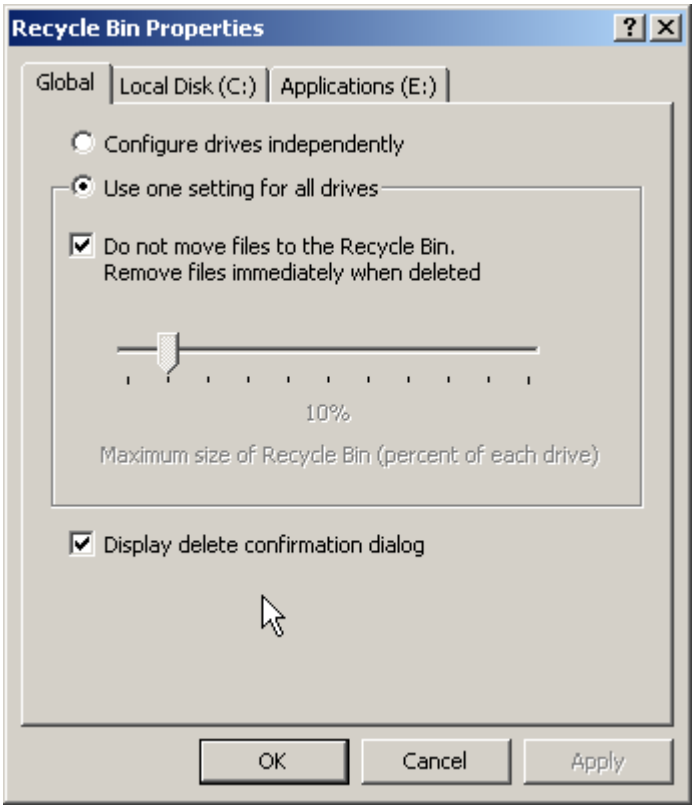

Figure 8-11. Set Recycle Bin to Auto-Delete All Files

8.4 Securing the Network Interface

A number of network protocols and components used by legacy Windows clients are installed by default on Windows 2000 Professional machines to provide instant backwards compatibility. It is recommended that users determine if these protocols are necessary; they can be disabled or uninstalled if they are not. If legacy Windows clients in the network make use of these components, then some type of security device (e.g., a firewall or Intrusion Detection System (IDS)) should be implemented.

Note: The **Internet Protocol (TCP/IP)** and **Client for Microsoft Networks** components are the only network components tested and installed in the NIST configuration. These components are the listed in the **General Tab** of **TCP/IP Properties** for your connection. Because of site-specific networking requirements additional network components may require installation. Please research the security ramifications of installing the components and uninstall or disable any network components not required.

Disable LMHOSTS lookup and disable tunneling of NetBIOS over TCP/IP if this service is not being used. If running a network connection with TCP/IP, open the **Properties** window of the local area network (LAN) connection and click on the **TCP/IP properties** button. From here, open the **advanced** properties window by clicking on the **advanced** button. After the Advanced TCP/IP Properties window has opened, click on the **WINS** tab to display the WINS properties for this connection, as shown in Figure 8-12.

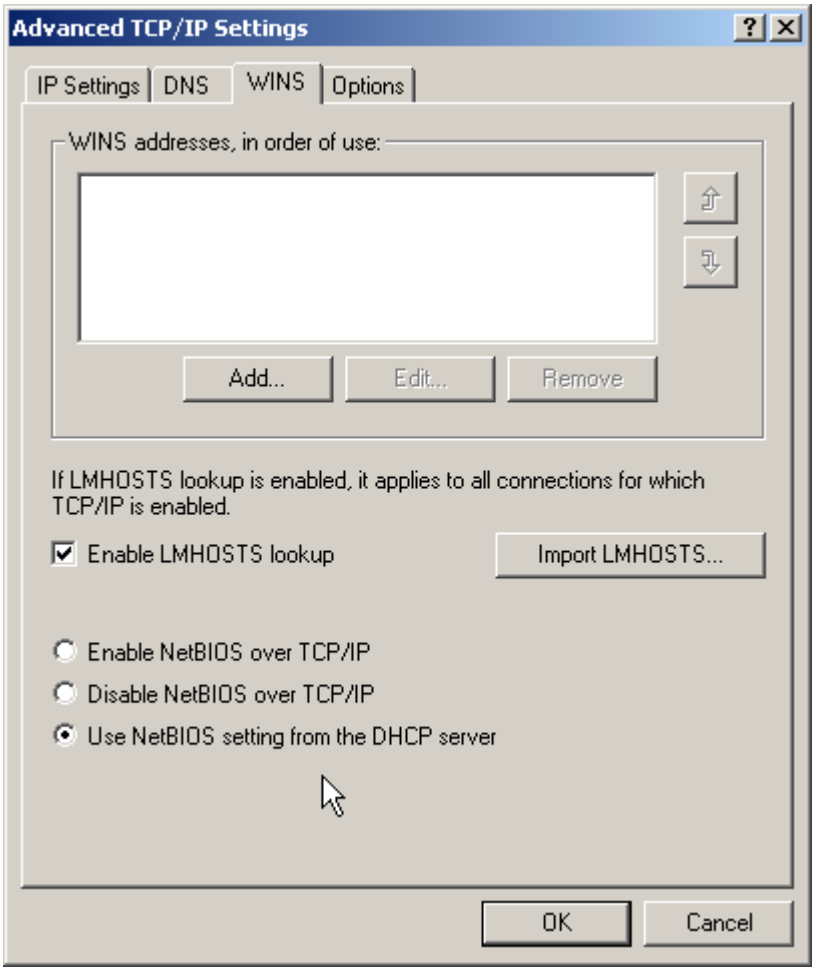

Figure 8-12. Disable LMHOSTS Lookup and NetBIOS Tunneling

Note: Windows 2000 uses NetBIOS over TCP/IP (NetBT) to communicate with prior versions of Windows NT and other clients, such as Microsoft Windows 95. Careful testing should be done before disabling NetBIOS over TCP/IP in any production environment. Programs and services that depend on NetBIOS no longer function after you disable NetBT services, so it is important that you verify that your clients and programs no longer need NetBIOS support before you disable it.

If the **Enable LMHOSTS lookup** checkbox is checked, uncheck it to disable LMHOSTS lookup. LMHOSTS is a resource used by legacy Windows clients for purposes of NetBIOS name identification.

If the network connection uses statically assigned networking information, ensure that the **Enable NetBIOS over TCP/IP** radio button is not checked. In Figure 8-12, this network connection obtains its network configuration from a Dynamics Host Configuration Protocol (DHCP) server. If this is true for your network, ensure that the DHCP server assigns connection information that disables this option.

NetBIOS is a nonroutable network protocol allowing some small amount of protection from external network access. When NetBIOS is allowed to be tunneled over TCP/IP, any network share or service, such as default Windows 2000 drive shares, can be accessed by the outside world. It is recommended that the enterprise perimeter firewall or border router block these ports tcp/udp 135 to 139 and 445. In addition, the Windows 2000 Professional systems that are not connected to the trusted and protected network should operate with properly configured personal firewall software to provide additional

protection. For further information about protecting systems connected to foreign network, refer to *NIST Special Publication 800-46, Security for Telecommuting and Broadband Communications*. The document is available at http://csrc.nist.gov/publications/nistpubs/.

8.4.1 TCP/IP Port Filtering

An additional security step that can be considered is enabling Windows 2000 TCP/IP port filtering. This step allows a custom definition of what incoming connections are allowed into the host computer while simultaneously allowing outgoing and established connections to work normally. This feature is best used on systems with a specialized function or an unchanging controlled software load.

Note: This built-in feature requires extensive onsite testing to access incoming ports that software installed on the workstation and the network environment the workstation resides in require. NIST does not specifically recommend the use of TCP/IP filtering. The preferred method of limiting access to a Windows 2000 workstation is IPsec filtering listed below.

8.4.2 IPsec Filtering

IPsec is designed to encrypt data as it travels between two computers, protecting the data from modification and interpretation. IPsec filtering can also be used to restrict and allow unencrypted traffic on specific ports. Using IP filtering, IPsec examines all IP packets for addresses, ports, and transport protocols. Rules contained in local or group policies tell IPsec to ignore or secure specific packets, depending on addressing and protocol information. By default, certain traffic is not filtered or protected by Windows 2000 IPsec; these kinds of traffic are known as the default exemptions and, minus Broadcast and Multicast, they only apply to IPsec transport mode filters:

- **Resource Reservation Protocol (RSVP)—**used for quality of service (QoS) of IP traffic. Required for QoS to work with Windows 2000.
- **Internet Key Exchange (IKE)—**IKE source and destination UDP port 500 traffic used in many VPN configurations.
- **Kerberos**—the main authentication protocol used in native Windows 2000 domain environments. Kerberos traffic uses a TCP and User Datagram Protocol (UDP) source and destination port 88.
- **Broadcast**—network traffic going from one sender to many receivers. Used for various networking functions.
- **Multicast**—traffic sent from one sender to multiple receivers in the address range of 224.0.0.0 to 239.255.255.255.

A registry value can be set to remove most of these exemptions and allow filtering on the above traffic; **HKLM\SYSTEM\CurrentControlSet\Services\IPsec\NoDefaultExempt** this DWORD value registry key can be set to 0 = default exemptions are still active or 1 = disable the exemption for RSVP and Kerberos in Windows 2000. Broadcast and Multicast cannot be restricted.

The steps to add or edit IPsec filters are listed below.

- In **IP Security** policies from the **Local Security Policy** tool, double-click the policy that you want to modify.

- Double-click the rule that contains the **IP Filter List** you want to modify.
- Do one of the following:
- If you are adding an IPsec filter list, on the **IP filter list** tab, click **Add**.
- If you are reconfiguring an existing **IP filter list**, double-click the **IP filter list**.
- In **IP Filter List**, do one of the following as shown in Figure 8-13:

To	Do This
Use the IP Filter Wizard to create a filter	Confirm that the **Use Add Wizard** check box is selected, and then click **Add**.
Create a filter manually	Clear the **Use Add Wizard** check box, then click **Add**.
Reconfigure an existing filter	Double-click the filter.

Figure 8-13. IP Filter List

- On the **Addressing** tab, select the **Source Address** as shown in Figure 8-14:

Select	To Secure Packets From
My IP Address	All IP addresses on the computer for which you are configuring this filter.
Any IP Address	Any computer.
A specific DNS Name	The Domain Name System (DNS) name that you specify in *Host name*. The DNS name is resolved to its IP addresses, and then filters are automatically created for the resolved IP addresses. This option is available only when creating new filters.
A Specific IP Address	The IP address that you specify in *IP Address*.
A Specific IP Subnet	The IP address that you specify in *IP Address* and the subnet mask that you specify in *Subnet Mask*.

Figure 8-14. Source and Destination Address

- Click **Destination Address** and repeat the previous step for the destination address.
- Under **Mirrored**, select the appropriate setting as shown in Figure 8-15:

To	Do This
Automatically create two filters based on the filter settings: one for traffic to the destination and one for traffic from the destination	Select the **Mirrored** check box.
Create a single filter based on the filter settings	Clear the **Mirrored** check box.
Create a filter for an IPsec tunnel	Clear the **Mirrored** check box. For IPsec tunnels, you must create two filter lists: one list describes the traffic to be sent through the tunnel (outbound traffic) and another describes the traffic to be received through the tunnel (inbound). Then, create two rules that use the inbound and outbound filter lists in your policy.

Figure 8-15. Mirror Filter Settings

- On the Description tab, in Description, type a description for this filter; for example, specify to what computers and traffic types it applies.
- If you require additional IP filtering by a specific protocol or port number, on the Protocol tab, configure advanced filter settings.

Figure 8-16 illustrates the use of the **Local Security Policy** tool to create a sample IPsec policy that blocks all protocols but allows common Internet traffic. In this example, the user of the local system is permitted to navigate the Web, connect to the printers, connect to the server message block (SMB) and file transfer protocol (FTP) file servers, ping other hosts, send and receive e-mail messages, and query the domain name service (DNS) server.

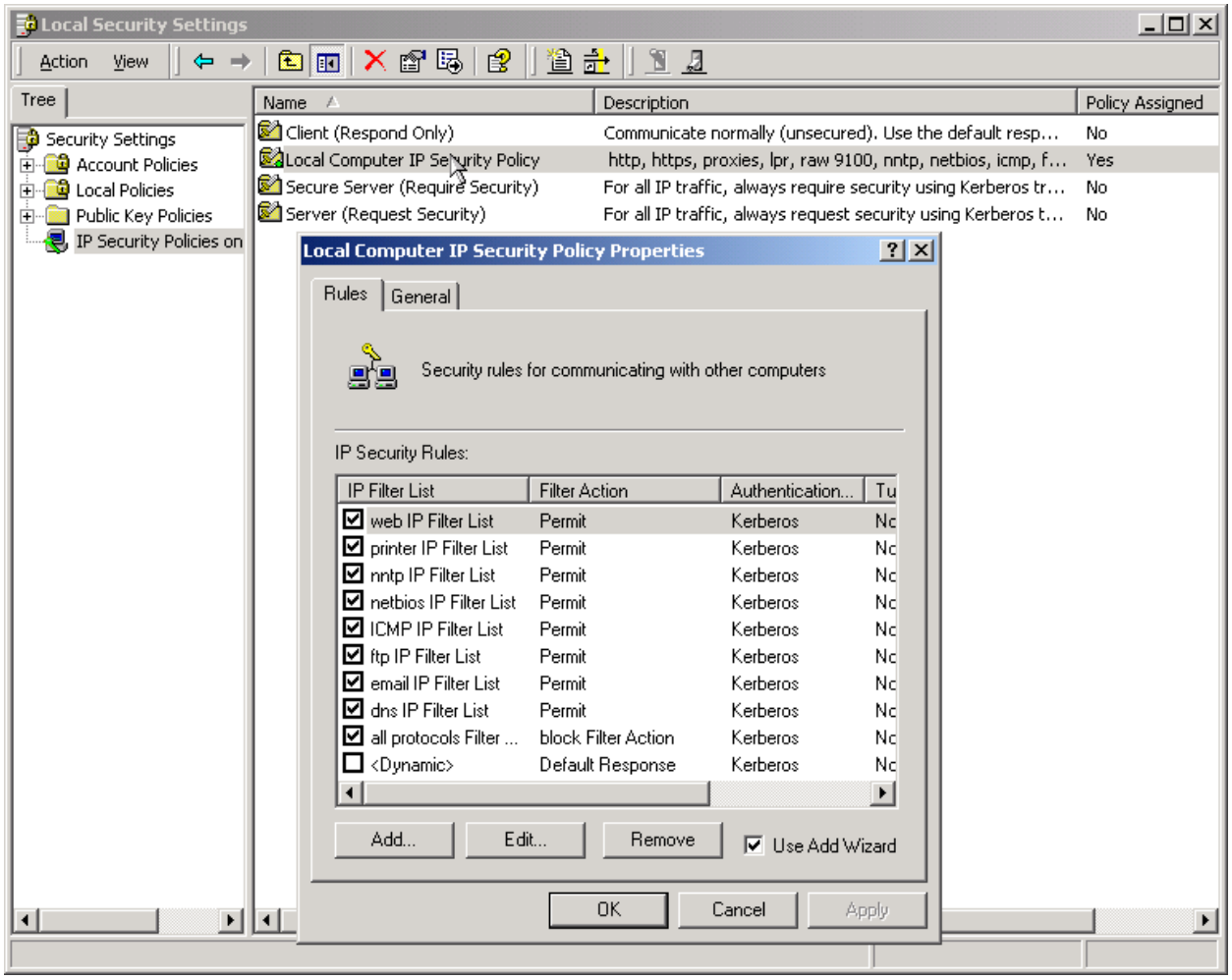

Figure 8-16. A Sample IPsec Policy

8.5 Disabling Unnecessary Services

Following the installation of Windows 2000 Professional, several services are configured to start automatically when the system boots. Many of these services are intended for machines running within a Windows 2000 domain and are not necessary for stand-alone workstations. Disabling a service is the simple process of changing its startup method from Automatic to Disabled within the Computer Management MMC snap-in, as shown in Figure 8-17.

Disabling a service is a rapid way to stop services from running on a Windows 2000 Professional workstation. Whenever possible, remove the unneeded services from the system by using the **Add/Remove Programs** control panel.

Note: Many services cannot be removed entirely and must be disabled to stop them from executing.

Once the **Service** window is open, double-clicking on a service will open its **Properties** window. From here, users can change the **Startup type** to **Manual** or **Disabled** and can press the service **Stop** button if the service is running.

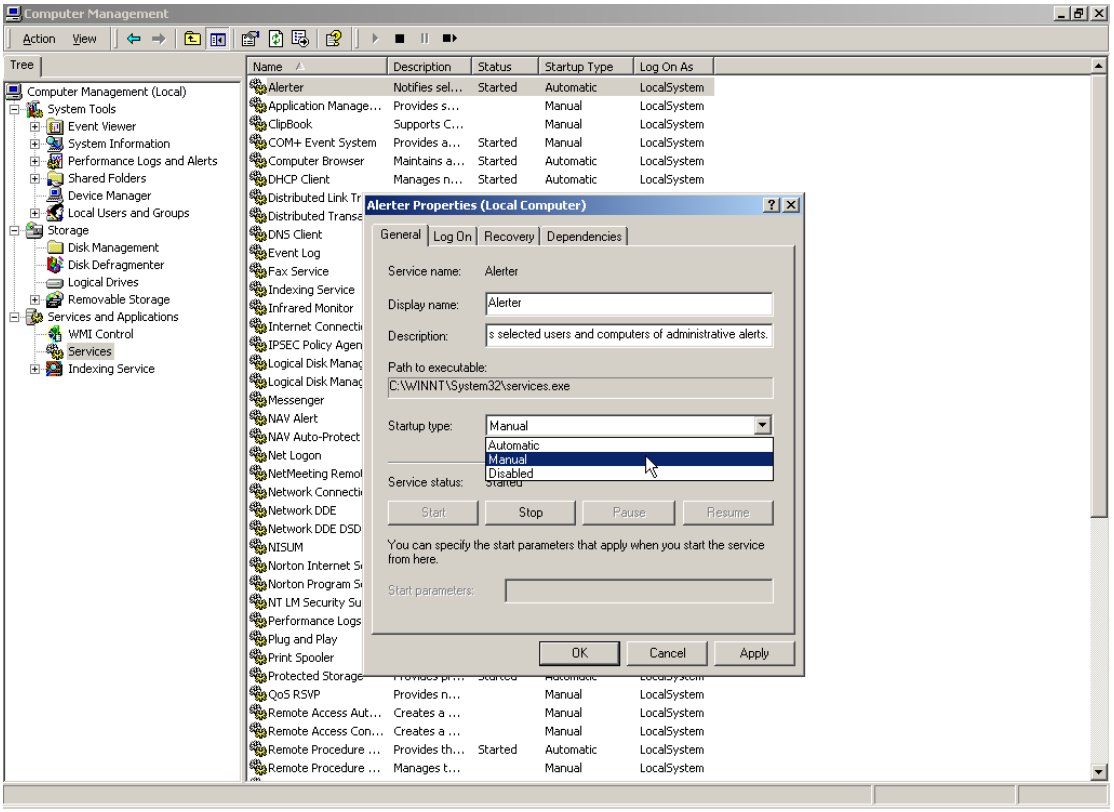

Figure 8-17. Disable Unnecessary Services

Table 8-1 lists services that can be disabled on a stand-alone Windows 2000 Professional machine, along with a description of each service. These settings are not defined in the NIST template found in Appendix B. Determine what settings are required for your environment and adjust the template before applying to your systems.

Table 8-1. Windows 2000 Professional Services

Service	Description
DHCP Client	Contacts a DHCP server to obtain a DHCP lease for network connection configuration. Disable this if network connections are statically configured.
Distributed Link Tracking Client	Provides configured notifications of NTFS networked file activity within a Windows 2000 domain. Disable this service if running a stand-alone machine.
Messenger	Sends alerts of various events to the console; useful within a Windows 2000 domain.
Remote Registry Service	Allows remote manipulation of Windows 2000 Professional registry. Disable this unless determined to be absolutely necessary.
RunAs Service	Enables programs to execute under a specified alias—for example, an Administrator can log on to a system as an unprivileged user as recommended and can execute administrative programs using the RunAs service. NIST recommends the use of this service.
Server Service	The SA should disable this service unless the Windows 2000 Professional workstation must share files. It is present if the File and Printer Sharing for Microsoft Network service is installed.

Service	Description
Alerter	Can send a network popup message and/or run a program when one of the Performance Monitor counters exceeds a preset threshold. Disable if you do not require this functionality.
Fax Service	Allows faxes to be sent and received; disable if not necessary.
Indexing Service	Indexes the entire all files on the system for rapid searching. Disable if you do not want this functionality.
Infrared Monitor	Enables infrared ports to function. Disable if infrared capability is not desired.
Logical Disk Manager Administrative Service	Service is started only when a disk is configured or partitioned. It is used to provide Administrative functions for Logical Disk Manager. Required to use the Disk Management user interface.
Net Logon	Used in Domain Member configurations. Do not disable if in a Domain.
Netmeeting Remote Desktop Sharing	Allows authorized remote users to connect to your desktop. Disable if this functionality is not required.
Performance Logs and Alerts	Used to configure Performance Logs and Alerts; also used to collect log and alert information. Disable if Performance Logging is not desired.
Remote Access Auto Connection Manager	Starts when no network connection is available and offers to dial up to connect when an application attempts to access the internet. Disable if this functionality is not required.
Remote Procedure Call (RPC) Locater	Provides name services for RPC clients. Disable if no third-party programs require this functionality.
Smart Card	Manages and controls access to smart cards. Disable if smart cards are not used in your system.
Smart Card Helper	Provides support for non-plug and play smart card readers. Disable if no non-plug and play readers will be installed on the system.
Uninterruptible Power Supply (UPS)	Manages serial communications with a UPS. Disable if not required.
Windows Management Instrumentation (WMI)	Provides system management information used by internal and external partners. Disabling this service will prevent management information applications from running.
WMI Driver Extensions	Tracks drivers that have WMI information to publish. Disable if WMI is disabled.
Windows Time	Used to access Network Time Protocol services. Disable if you do not require an external time source.
Utility Manager	Used to provide rapid access to accessibility tools: Magnifier, Narrator, and On-Screen Keyboard. Disable if rapid access to these tools is not required.

8.5.1 Windows 2000 Professional Services

Note on Applying the Security Template: The security template **NISTWin2kProGold.inf,** fully defined in Appendix B and provided as a separate file to this document, has been customized to provide optimum security for a Windows 2000 Professional computer. It is recommended that Administrators review Appendix B to ensure all settings provided by the **NISTWin2kProGold.inf** template are appropriate for their specific environment. Copy the **NISTWin2kProGold.inf** file into the directory **C:\winnt\security\templates**.

Note: Before applying the template, open the **Local Security Policy** node and export the currently running local policy (see Section 4.5). The exported policy will allow you to restore most of the currently running settings if needed. Many of the default settings in the exported template will be listed as not defined; if the settings are defined in the NIST template, they will not be changed back to default if the

backup template must be applied. It is extremely important to test the template settings in a laboratory environment before wide-scale deployment.

To apply the security template using **secedit.exe**, type the following syntax at the command prompt:
C:\>secedit /configure /db C:\winnt\security\NISTWin2kProGold.sdb /cfg C:\winnt\security\templates\NISTWin2kProGold.inf

This syntax, entered on one line, will apply the security settings specified in the security template **NISTWin2kProGold.inf.** The secedit.exe utility will create a log of its actions when the task is complete. This log file is usually stored in the **%SystemRoot%\security\logs** folder. Note that the same task can be achieved using the **Security Configuration and Analysis MMC** snap-in described in Section 4.2.

When the system configuration is complete, follow the guidelines in Section 6.3 to create the ERD for the system and perform a full backup on removable media. Use the backup program included in a default Windows 2000 Professional installation found in **Programs | Accessories | Backup** or a third-party backup program for this initial full backup. Continue regular backups throughout the life cycle of the system in accordance with local policy. Examples of occasions for backups outside the established backup cycle include application additions, OS modifications, updating, and patching. Ensure user data is backed up regularly and test recovering a set of files from the backup archive. For more information about system backups and disaster recovery, refer to http://support.microsoft.com/default.aspx?scid=kb;EN-US;q287061.

Note: Backups over unencrypted network links are subject to eavesdropping.

8.6 Domain Member Machine Configuration

The principles discussed in Section 8 can be applied to Windows 2000 Professional domain members and stand-alone workstations. The differences between stand-alone and domain member workstations are in the method of authentication (Kerberos; refer to Section 2.1) and method of security policy deployment (Active directory **Group Policy;** refer to Section 4.3).

Note: Test the security templates in each OU before deployment throughout the enterprise.

8.7 Summary of Recommendations

- Secure the System and Data Partitions and restrict access to critical system files and utilities. Refer to Appendix B for specific recommended settings.
- Replace Everyone Group with Authenticated Users.
- Enable EFS to encrypt sensitive data at the folder or directory level.
- Remove the OS2 and POSIX system files.
- Disable Memory Dump.
- Set Recycle bin to Automatically Delete files.
- Disable LMHosts Lookup.
- Disable NetBIOS over TCP/IP when appropriate and block the tcp/udp 135 to 139 and 445 ports at the perimeter firewall or border router.

- Use personal firewall software to protect the systems connected to untrusted networks.
- Enable TCP/IP Filtering when possible.
- Enable IPsec Filtering when possible.
- Disable Unnecessary Services. Refer to Appendix B for specific recommended settings.
- Apply the NIST Security Template.
- Perform a backup of system data after any system modifications.
- Perform backups of user data on a regular schedule and test recovering from the backup archives.

9. Administrator, Power Users, and Users

Windows 2000, upon installation, provides six default built-in groups: Administrators, Power Users, Users, Replicator, Guests, and Backup Operators. Windows 2000 also includes some special groups, such as the Everyone and Authenticated Users group. The Windows 2000 Professional Administration model is based on assigning individual users into groups to control the system access rights of those users. This organizing principle reduces the Windows 2000 Professional administrative burden by classifying large numbers of users into smaller group account areas. Then the group account areas are assigned rights to individual resources. It is recommended that the individual user's home directory be the only resource assigned to the user. The groups are described below:

- **Administrators group** can perform any action on any registry or file system object; any right that is not assigned by default to the Administrators group can be self-assigned by the Administrators group. In addition, any custom right that the Administrators do not have by default, they can grant to themselves.
- **Power Users group** is an insecure group designed to provide backward compatibility for applications that are not certified for Windows 2000 and to perform basic administrative tasks in a Windows 2000 Professional workgroup environment.
- **Users group** drastically limits the ability of one user to affect any other user on the system. It has default privileges to operate and use any program preinstalled on the Windows 2000 Professional computer. The group also has default read access to many file areas on a Windows 2000 Professional computer.
- **Replicator group** is used for adding the special domain user that will log on to the domain replicator service functions; no other users should be added to this group.
- **Guests group** was created to allow restricted anonymous access to a Windows 2000 workstation and is disabled by default.
- **Backup Operators group** by default has all the privileges necessary to backup and restore all files on a Windows 2000 workstation.
- **Everyone group** by default contains all users who authenticate to the domain; the group membership cannot be directly controlled by the SA.
- **Authenticated Users group** is used as a more secure replacement for the Everyone group and contains all users who authenticate to the domain minus anonymous users and guests; Administrators cannot directly control membership to this group.

The following sections discuss three of the groups (Administrators group, Power Users group, and Users group) in detail, including out of the box permissions and capabilities, by first introducing how Windows 2000 Professional handles user accounts internally. Many of these default settings are changed by the templates provided with this document. The section describes additional steps that can be taken to ensure proper account usage and safety, including how to assign a user account to a certain group or groups. In addition, it introduces the recommended account policies and user rights assignment reflected in the NIST templates.

9.1 Windows 2000 Security Identifier

Windows 2000 Professional is designed to assign a unique identifier to each user account, called a security identifier (SID). A SID is a binary value that is set for a user account by the system when the account is created. A SID identifies a security principal (user, group, or machine account) on a Windows 2000 machine. The SID is used when a Windows 2000 system account, process, or user attempts to access a resource within the OS. Windows 2000 compares the principal's SID with the discretionary access control list (DACL) of the resource.

The DACL is more commonly referred to simply as an access control list, or ACL. If the principal's requested action matches the ACL permission, then access is granted. Well-known SIDs are common to all installs of Windows 2000 and identify generic users or generic groups. Information about these generic SIDs can be found in Microsoft Support article number Q243330: http://support.microsoft.com/support/kb/articles/Q243/3/30.ASP

9.2 Administrators Group

In Windows 2000 Professional, the Administrator account is a member of the Administrators group and is configured with a SID in the following format:
S-1-5-<Number>-< Number >-< Number >-500

The trailing number of **500** indicates that the SID corresponds to a local or domain Administrator account. An Administrator account should be used ONLY for tasks like those below:

- Installing, removing, or troubleshooting hardware components.
- Installing Windows updates/service packs/hotfixes.
- Installing and repairing Windows OS.

9.3 Power Users Group

Any application not Windows 2000 compliant is considered a "legacy application." Only Power Users and Administrators can run legacy applications under Windows 2000. For a list of applications that are certified for Windows 2000, see http://www.veritest.com/certified/win2000server/DesktopApps.asp.

Power Users can accomplish the following:

- Install and remove applications per computer that do not install system services.
- Customize systemwide resources (for example, System Time, Display Settings, Shares, Power Configuration, and Printers).
- Create local users and groups.
- Modify users and groups that they have created.
- Create and delete non-admin file shares.
- Create, manage, delete, and share local printers.

Power Users are not permitted to access other users' data stored on an NTFS partition. In practice, Power Users cannot install many legacy applications because these applications attempt to replace operating

system files during their setup process. Table 9-1 lists the **default access control settings** for Users and Power Users that are applied to file system objects during a normal installation of Windows 2000 Professional. The following syntax rules apply:

- %SystemDir% refers to %windir%\system32
- *.* refers to the files and not directories contained in a directory
- RX means Read and Execute.

Table 9-1. Default Access Control Settings for File System Objects

File System Object	Default Power User Permissions	Default User Permissions
c:\boot.ini	RX	None
c:\ntdetect.com	RX	None
c:\ntldr	RX	None
c:\ntbootdd.sys	RX	None
c:\autoexec.bat	Modify	RX
c:\config.sys	Modify	RX
c:\Program Files	Modify	RX
%windir%	Modify	RX
%windir%*.*	RX	RX
%windir%\config*.*	RX	RX
%windir%\cursors*.*	RX	RX
%windir%\Temp	Modify	Synchronize, Traverse, Add File, Add Subdir
%windir%\repair	Modify	List
%windir%\addins	Modify (Dir\Subdirs) RX (Files)	RX
%windir%\Connection Wizard	Modify (Dir\Subdirs) RX (Files)	RX
%windir%\fonts*.*	RX	RX
%windir%\help*.*	RX	RX
%windir%\inf*.*	RX	RX
%windir%\java	Modify (Dir\Subdirs) RX (Files)	RX
%windir%\media*.*	RX	RX
%windir%\msagent	Modify (Dir\Subdirs) RX (Files)	RX
%windir%\security	RX	RX
%windir%\speech	Modify (Dir\Subdirs) RX (Files)	RX
%windir%\system*.*	Read, Execute	RX
%windir%\twain_32	Modify (Dir\Subdirs) RX (Files)	RX
%windir%\Web	Modify (Dir\Subdirs)	RX

File System Object	Default Power User Permissions	Default User Permissions
	RX (Files)	
%systemdir%	Modify	RX
%systemdir%*.*	RX	RX
%systemdir%\config	List	List
%systemdir%\dhcp	RX	RX
%systemdir%\dllcache	None	None
%systemdir%\drivers	RX	RX
%SystemDir%\CatRoot	Modify (Dir\Subdirs) RX (Files)	RX
%SystemDir%\ias	Modify (Dir\Subdirs) RX (Files)	RX
%SystemDir%\mui	Modify (Dir\Subdirs) RX (Files)	RX
%SystemDir%\OS2*.*	RX	RX
%SystemDir%\OS2\DLL*.*	RX	RX
%SystemDir%\RAS*.*	RX	RX
%SystemDir%\ShellExt	Modify (Dir\Subdirs) RX (Files)	RX
%SystemDir%\Viewers*.*	RX	RX
%SystemDir%\wbem	Modify (Dir\Subdirs) RX (Files)	RX
%SystemDir%\wbem\mof	Modify	RX
%UserProfile%	Full Control	Full Control
All Users	Modify	Read
All Users\Documents	Modify	Read, Create File
All Users\Application Data	Modify	Read

9.4 Users Group

Within Windows 2000 Professional, any account classified as a User is designed to allow the use of the Windows 2000 Professional computer and nothing more. If Windows 2000 Professional is installed on an NTFS partition, the default security settings are designed to prevent User level accounts from compromising the integrity of the operating system. For example, system-critical directories and program files are controlled with default NTFS ACL configurations, and access to editing the Windows registry is prohibited by Users. Users cannot by default impersonate other users to install unsafe software or access their private data. This illustrates two important and additional steps to take concerning User level accounts:

- Ideally, all end-users of Windows 2000 Professional should belong to the Users group ONLY.
- End-users applications should be deployed with properly configured ACLs.

A member of the Users group should in theory be able to run any application installed previously by an Administrator, Power User, or other user. In practice, users will be unable to execute legacy Windows applications because these applications were designed under a previous version of the Windows kernel

and without considering Windows 2000 OS security. Users may also have difficulty executing some Active X controls.

9.5 Change Account Group Membership

Account management is an important process in securing Windows 2000 Professional. One important step in managing user accounts on Windows 2000 is determining group membership. This section describes how to access the account management applet on Windows 2000 Professional and how to change the group membership for a particular account.

To open the Local Users and Groups management applet, open the **Computer Management MMC** applet from **Start | Settings | Control Panel**. Double-click on the **Local Users and Groups** icon from the list on the left as shown in Figure 9-1.

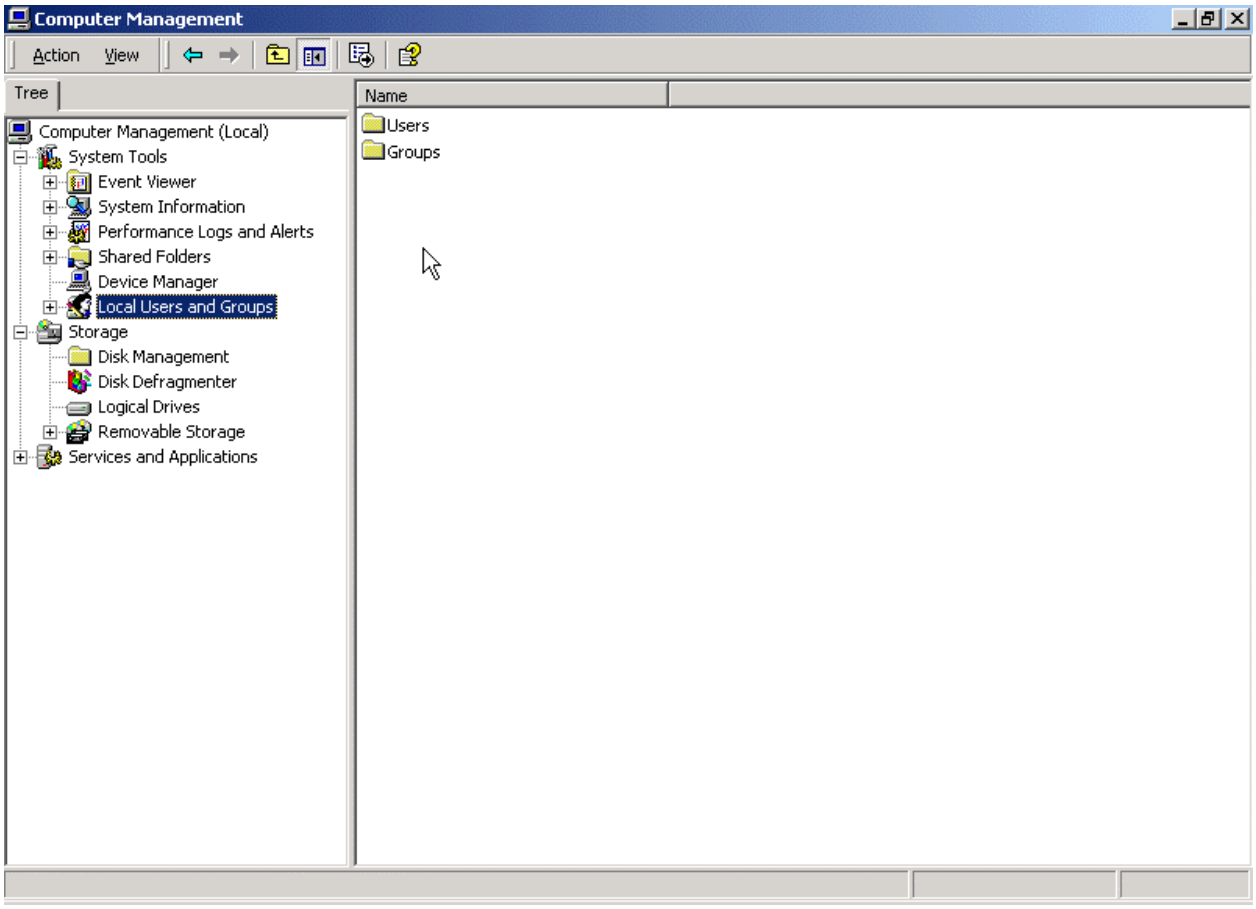

Figure 9-1. Open Local Users and Groups from Computer Management

This action opens the User Management applet, which allows control over the accounts properties. As shown in Figure 9-1, to access the account properties for a specific user, double-click on the **Users** folder icon on the right. This opens the list of accounts that have been installed. To access the account properties for any one of the accounts, choose an account and right-click on it to open the context menu

for that account. From this menu, choose **Properties** to open the account properties dialog box for that account as shown in

Figure 9-2. Double-clicking on the specific user icon can open the same properties window. In Figure 9-2, the **Member Of** tab is showing that the user is a member of the Administrators group.

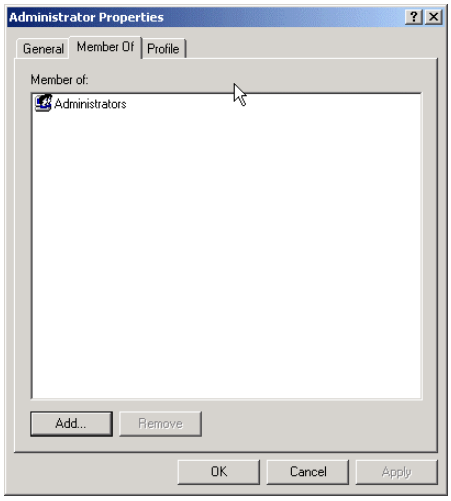

Figure 9-2. Account Properties Box for Example Account Client

To add this user to a particular group, click on the **Add** button to open the **Select Groups** window. Choose the group to add from the top window, click on the **Add** button, and choose **OK** to close the **Select Groups** Window. Figure 9-3 shows the example user being added to a built-in group.

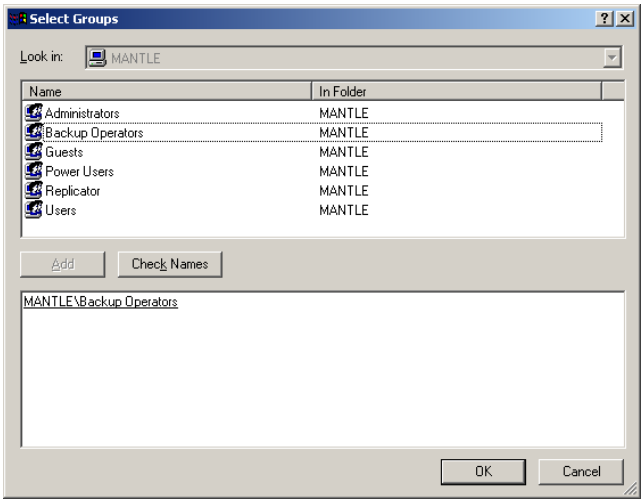

Figure 9-3. Adding a User to a Group

9.6 Account Policies

The NIST templates contain the NIST recommended password policy settings as shown in Figure 9-4. These settings can be modified to reflect your sites existing password policy before applying to your

system. The **Enforce Password History** section ensures that users do not "change" the password back to a password they have used before. The **Maximum password age** ensures that users change their passwords on a regular basis. The **Minimum password age** ensures that users cannot cycle through various passwords to override the history settings. **Minimum password length** ensures that the password will be difficult to break if an encrypted copy of it is obtained. **Passwords must meet complexity requirements** ensures that the password does not contain all or part of the user's account name, is at least eight characters long, and contains characters from three of the following four categories: English upper case characters (A-Z), English lower case characters (a-z), Base 10 digits (0-9), and nonalphanumeric (such as !,$#,%). If **Store passwords using reversible encryption for all users in the domain** is enabled, then the passwords are stored on the system in clear text versions; this setting should never be enabled.

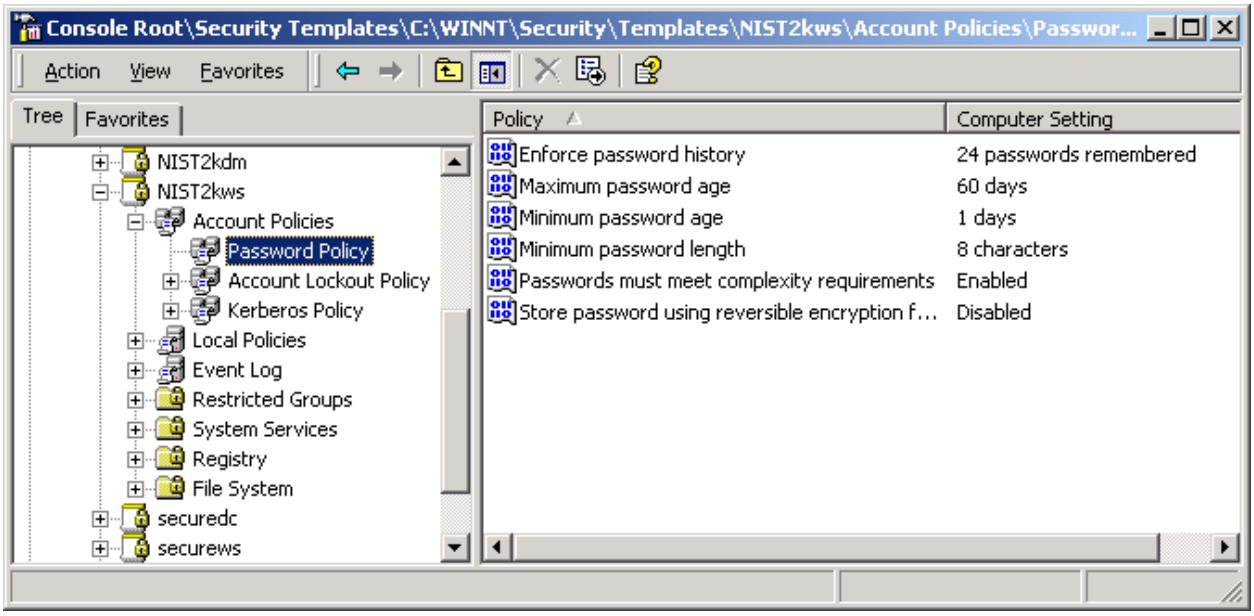

Figure 9-4. NIST Template Password Policy

9.7 Summary of Recommendations

- Use a logon account with User group permissions for day-to-day account usage.
- Use the Administrator account only when modifying or managing the system.
- Apply the NIST template to configure the user rights assignment, account password policy, and account lockout policy. Refer to Appendix B for specific recommended settings.
- Formulate a plan for dealing with ActiveX controls that cannot be downloaded under the secure User context. See Microsoft bulletins Q240897, Q241163, and Q280579.
- Never log on with administrative privileges unless you need to perform administrative tasks. Use the runas.exe command instead.

This page intentionally left blank

10. Application-Specific Configuration

This section addresses the application specific configuration tasks for Windows 2000 Professional commercial off-the-shelf (COTS) products. Many widely used applications in the federal and private sectors are discussed. Application configuration tends to involve numerous different tasks, from editing the registry to choosing locations to install products. Because several of the applications below address changes to the Windows 2000 registry, it is important to reiterate the necessity of maintaining a functional backup copy of the registry in case of an error. Specific instructions regarding how to back up the Windows 2000 registry can be found in Section 6.4.

The application types that will be discussed are electronic mail (e-mail) clients, Web browsers, productivity applications, and antivirus scanners. This list is by no means a complete list of applications to install on Windows 2000 Professional, nor does it imply any type of commercial endorsement of COTS products. The information presented in this section assumes that the reader has a moderate knowledge of the process of installing applications on the Windows platform. In this section, no keystroke-level descriptions are presented for every installation process. During the installation process, some details are provided when confusing steps are encountered to help the user.

Much of the following security discussion focuses on viruses, worms, Trojan horses, and other types of malicious code. This section presents recommendations that can be adopted to protect the system from malicious code while using these applications. To maintain consistency, whenever the discussions refer to any of these types of viruses or worms, the term "malicious code" will be used. For further information about active code, please refer to the *NIST Special Publication 800-28, Guidelines on Active Content and Mobile* Code, available at http://csrc/publications/nistpubs/

.

The **NISTWin2kProGoldPlus.inf** security template provides some additional protection from mobile code and Trojans by restricting access to standard command line tools that are many times exploited to gather network information or launch malicious code. The security template will deny **Users Group** access to many standard command line tools. This will reduce usability for the small portion of users that use the command line tools. It is very possible that a large portion of users may never realize that access to the tools has been denied, since they use the GUI and never the command line.

10.1 AntiVirus Scanners

Perhaps one of the more important software titles for every type of Windows 2000 machine, the importance of antivirus software cannot be emphasized enough. Although several competing product titles are available, the theory behind configuration and maintenance of antivirus scanners is independent. It is recommended that every Windows 2000 system operate with updated and properly configured virus scanner software. In addition, the host should be scanned regularly to verify that the file system is not infected with a virus.

Most antivirus software includes the following features:

- **Automatic Protection**—designed in part to scan critical system components such as startup files, system BIOS, and boot records. When an application attempts to modify one of these critical components, the auto-protection feature alerts the users and allows them to act accordingly. This feature also is watching the real-time activities of the computer and operating system to check for suspicious activity.

- **Disk Scanning**—scans all files on a hard disk for known viruses.
- **E-mail-Scanning**—scans e-mail attachments for known viruses.
- **Automatic Updating**—enables the user to connect to the manufacturer's site for automatic updates of virus definition files.

Each component is important and should neither be ignored nor disabled unless necessary. Although the inherent risk behind virus scanning technology is that it only intercepts known viruses (to the most current date of the virus data files), this does not diminish the importance of the software. A virus, which originates in some remote part of the world, could potentially take days to propagate halfway around the world.

10.1.1 McAfee Virus Scan

McAfee, a product of Network Associates (NAI), is sold as a stand-alone product or a member application of McAfee Office. The McAfee homepages are as follows:

- http://www.mcafee-at-home.com – for home users
- http://www.mcafeeb2b.com – for corporate users.

NAI has also developed an ActiveX version of McAfee called Virus Scan Online, which is located at http://www.mcafee.com. Users have the option of purchasing a CD copy of McAfee or to purchasing online and downloading from mcafee.com. This discussion focuses on McAfee Virus Scan installed with McAfee Office. The installation process of McAfee is straightforward. Proper configuration, however, is necessary following the installation/reboot procedure.

It is likely that the virus data files installed by default with the installation media are outdated; therefore, the data files should be updated before installation or even scanning the system for the first time. To update McAfee data files, start the **VScan Central** application from the **Start** menu. Once the **VScan Central** window opens, click on the **update** button at the bottom of the window, as shown in Figure 10-1.

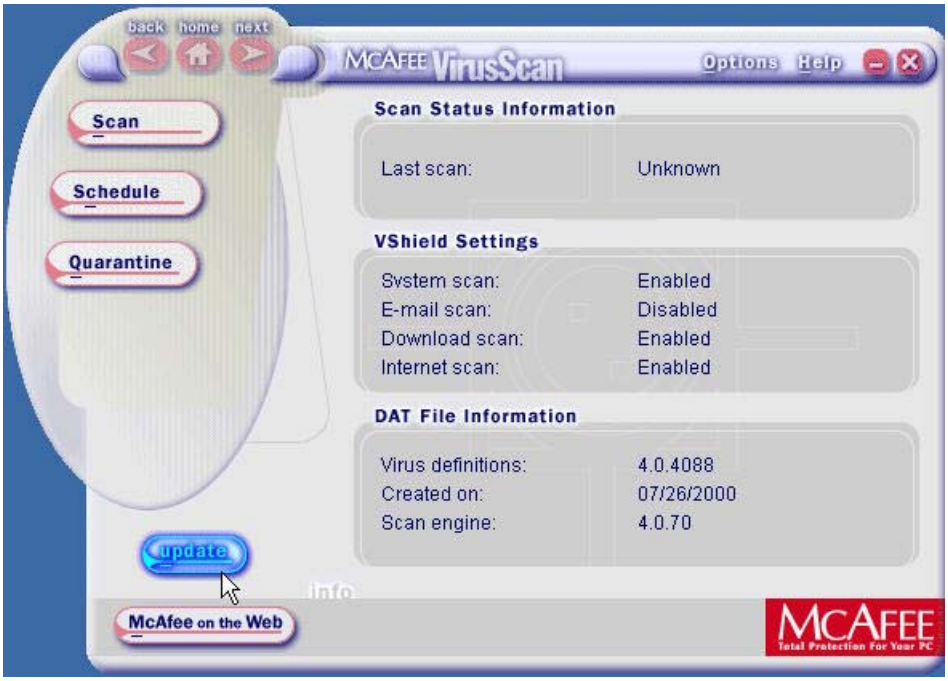

Figure 10-1. Update McAfee Virus Scan

This process starts the update utility SecureCast, which downloads and installs the newest data files for McAfee, as shown in Figure 10-2. SecureCast will not allow updates to McAfee unless proper registration information has been submitted.

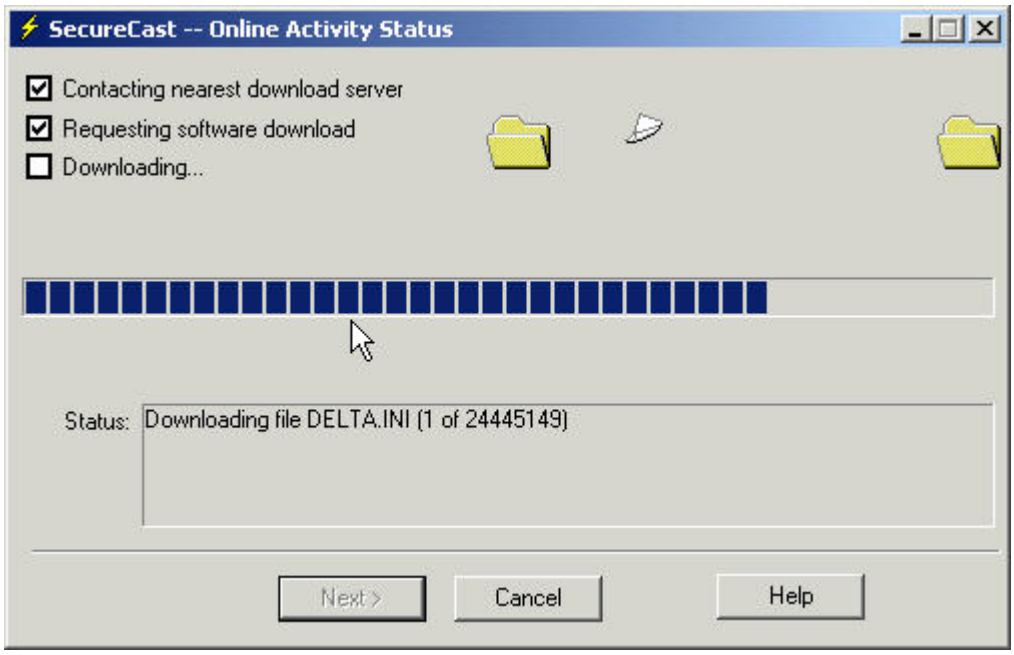

Figure 10-2. McAfee Virus Scan Update in Progress

Once the system has rebooted following the installation and any necessary updates of McAfee Virus Scan, it is important to configure the various options of McAfee, such as e-mail scanning and Internet

filter, and to password protect all settings. These options are configured from the **Virus Scan** options window. To configure e-mail scanning, see Figure 10-3, open the options window; then, click on the **E-Mail Scan** option in the list on the left side.

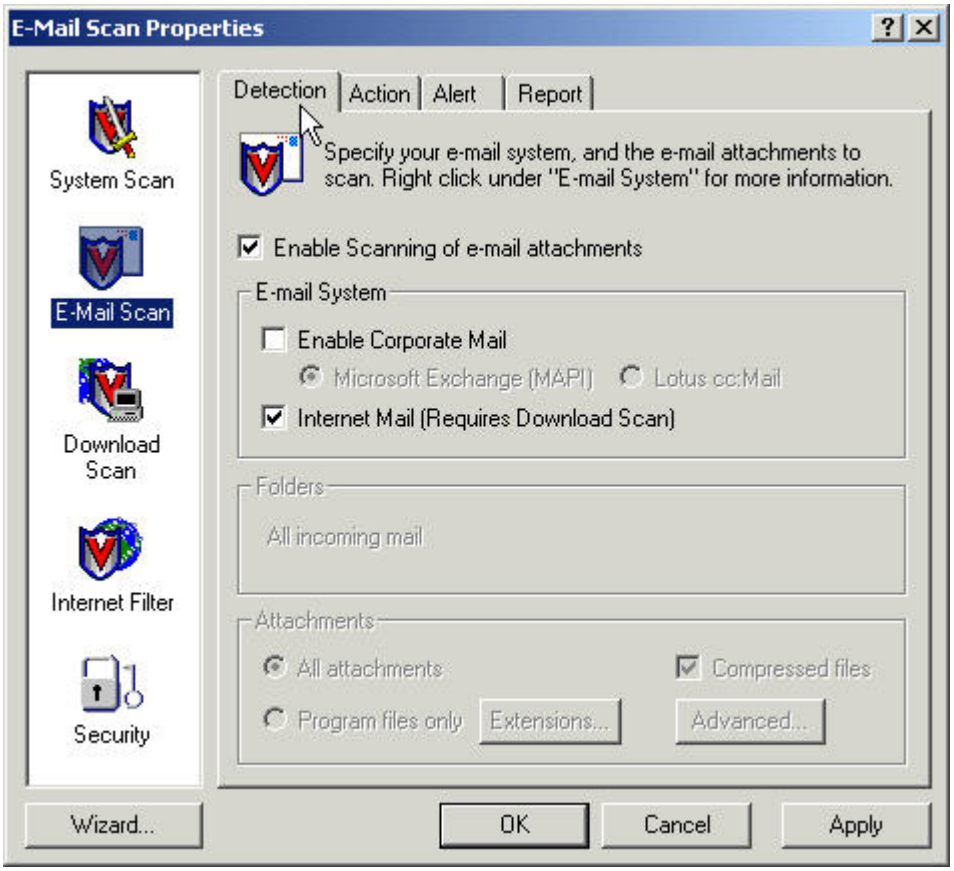

Figure 10-3.Configure McAfee E-mail Scanning

To determine the type of e-mail used by your organization, click on the **Enable scanning of e-mail attachments**, and check the appropriate mail type: Internet or Corporate Mail. If unsure of the mail type, click the **Internet Mail** option. This action will require that the McAfee download scan be enabled as well.

Similar to many other antivirus titles, McAfee is built with a virus heuristics setting designed to proactively search for virus-like behavior. This setting can be configured for each of the supported scan types. Although no exact prevention success rate is known for heuristic scanning, enabling this feature is recommended. To enable heuristics for e-mail scanning, click on the **Advanced** button at the bottom in the **E-Mail Scanning Properties** window.

It is also recommended that the **Internet Filter** be enabled. Once enabled, the default configuration options are sufficient for most organizations. The last recommended step is to enable password protection for these settings in the **Security** option, the last choice on the list on the left. To enable password protection, click on the **Security** option and check the **Enable Password Protection** checkbox shown in Figure 10-4. Any time that the user wants to change an additional property from this window, they must now supply a password.

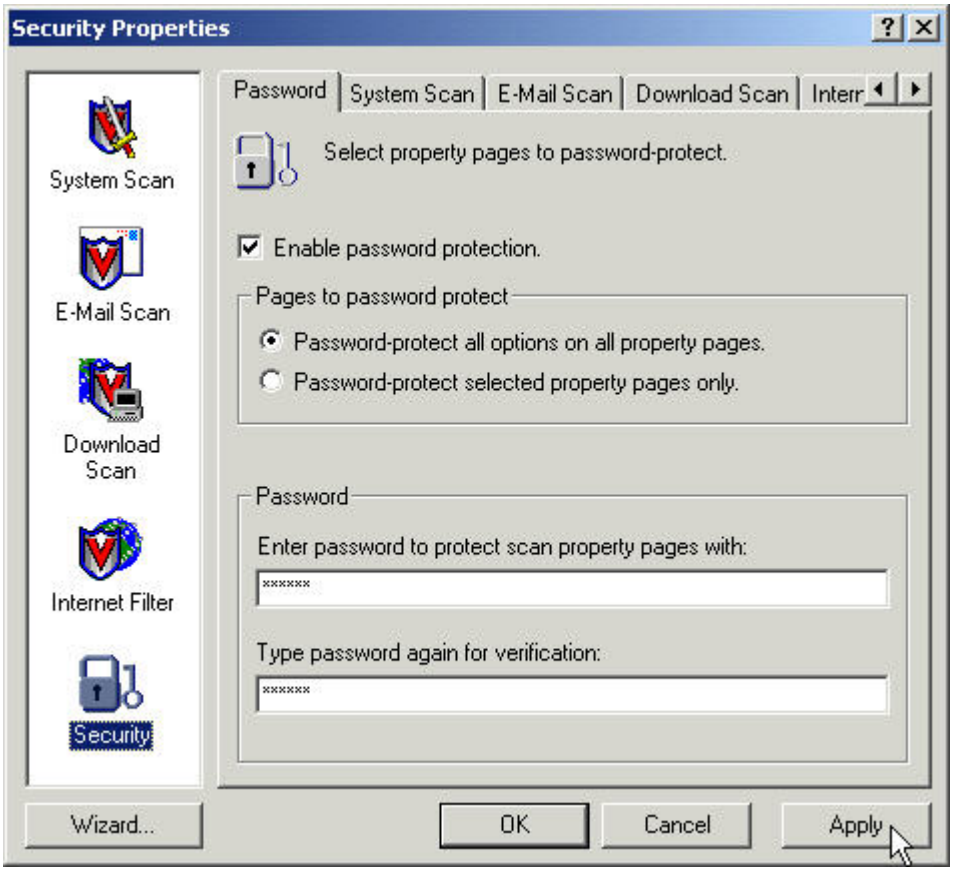

Figure 10-4.Configure McAfee Settings Password Protection

10.1.2 Norton AntiVirus

Norton AntiVirus comes in different versions, including stand-alone and corporate edition. If using Norton AntiVirus stand-alone, it is recommended that the following settings be changed from the default version: change bloodhound heuristics level to high; enable e-mail scanning, enable automatic live-update; and set file-system scan to include all types of files, not just program files. Live Update is the Symantec technology to install updates to the components of Norton AntiVirus.

Norton's method of proactively searching for virus-like activity is called the bloodhound detection. For safety reasons, it is recommended that this level be set at its maximum. To set the bloodhound level, perform the following:

- Open the **Norton AntiVirus auto-protect** window from the task bar.
- Click on the **Options** button at the top of the window to open the Norton AntiVirus options.
- Expand the **Auto-Protect** setting on the left side of the option window, and click on the **Bloodhound** choice. Ensure that the **Enable Bloodhound heuristics** checkbox is checked and that the **sensitivity level** is set to the **Highest level of protection** as shown in Figure 10-5.

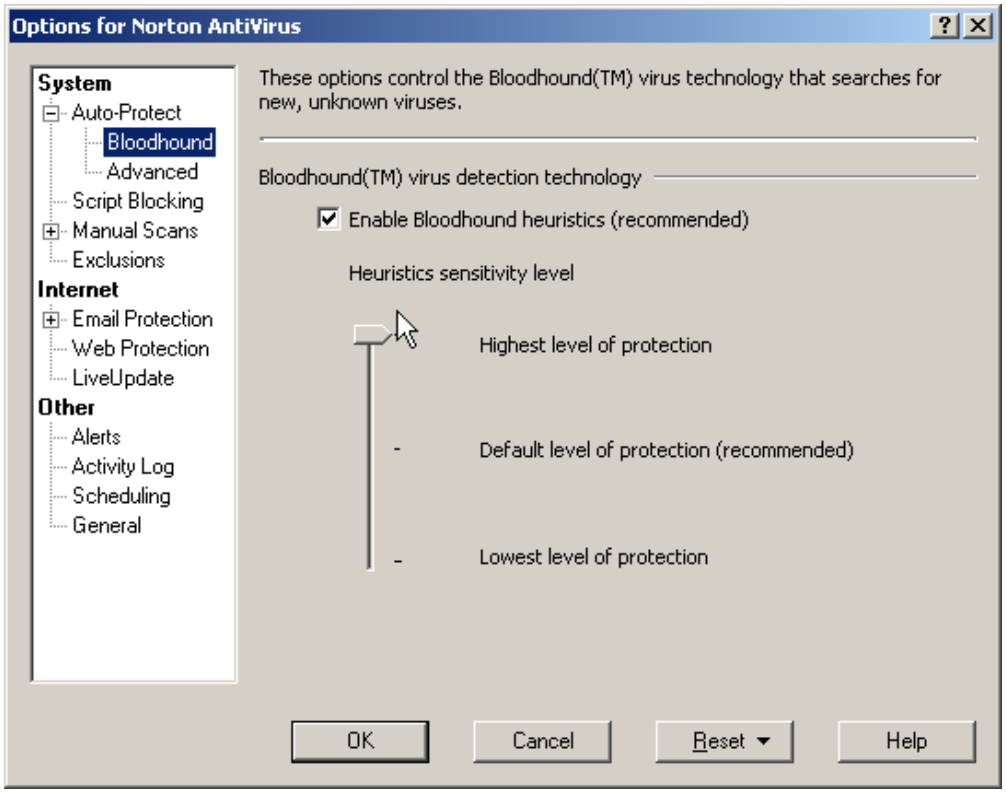

Figure 10-5. Set Norton AntiVirus Bloodhound Detection Levels

To ensure that Live Update will constantly check for updates to the virus signatures and Norton AntiVirus itself, automatic Live Update should be enabled. To enable automatic Live Update, perform the following steps:

- Open the **Options** screen again as in the previous example.
- Click on the **Live Update** option.
- Ensure that the Enable **Automatic Live Update** checkbox is checked.
- Below this checkbox, ensure that the first radio button is selected which says **Apply updates without interrupting me**.

This action is shown in Figure 10-6. It is important to know the manual method to check for and install updates to Norton AntiVirus. To run **Live Update** manually, click on the **Live Update** button located to the left of the **Options** button on the Norton AntiVirus main screen.

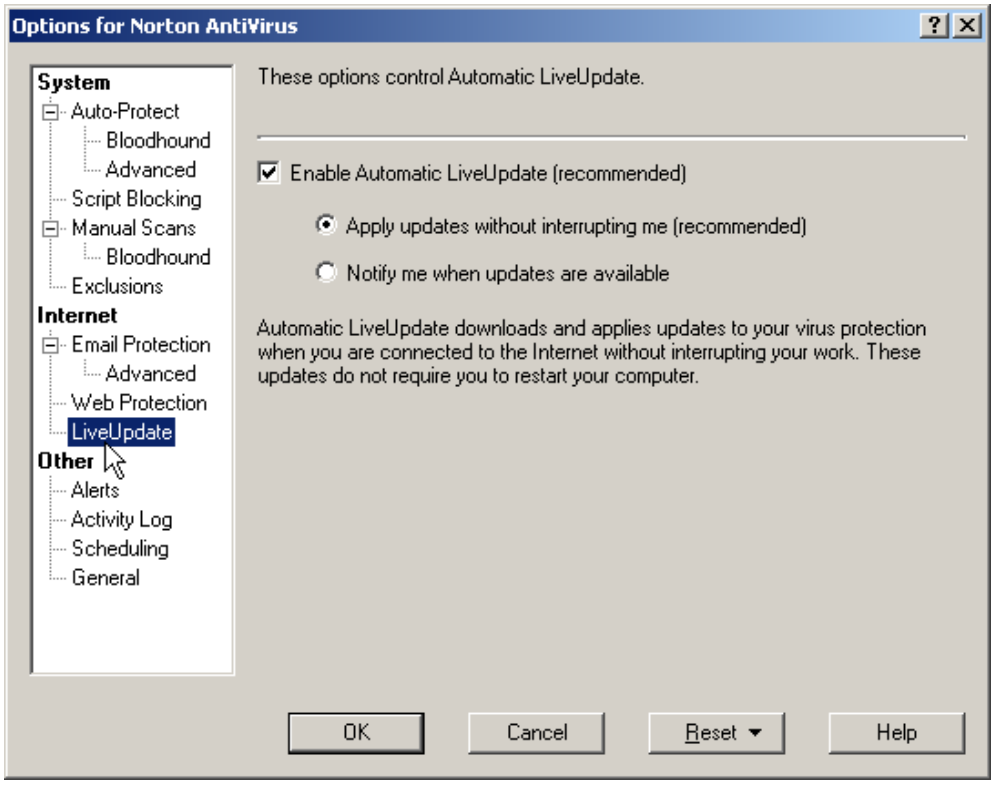

Figure 10-6. Set Norton AntiVirus Automatic Live Update

To enable Norton AntiVirus to scan incoming mail messages, the e-mail client must not be executing. This feature is available with the stand-alone version of Norton AntiVirus. To enable scanning of e-mail, perform the following:

- Open the Norton options screen as in the previous example.
- Expand the **E-mail Protection** option.
- The e-mail accounts detected will be listed in the box on the right side of the window. Check all accounts that will be protected, and click **OK** to proceed.

Once this step is performed, Norton AntiVirus will alert the user with a confirmation dialog box reminding the user that the e-mail client detected must not be running at this time. If this action is successful, close the options screen and return to the main Norton AntiVirus screen. If the e-mail status option is clicked, Norton should report that e-mail accounts are protected.

Note: The actual binary on the system that scans the messages for Norton AntiVirus stand-alone edition is called **poproxy.exe**. This binary runs continuously while e-mail scanning is enabled, so be aware of the added overhead. It is normal for this binary to appear in the process list or shows activity in system log files.

10.1.3 F-Secure Anti-Virus

F-Secure Anti-Virus, a product of the F-Secure Corporation, is available online from https://europe.f-secure.com/products/antivirus/

The current version of F-Secure is 5.30, which does not provide any e-mail scanning capabilities. The installation process has no reported problems and can install with default settings provided enough space exists on the partition. Once installed, just as with other antivirus software, it is recommended that real-time protection be enabled. To enable real-time protection, double-click on the **F-Secure** icon in the system tray. This action opens the **F-Secure Anti-Virus** options window, as shown in Figure 10-7.

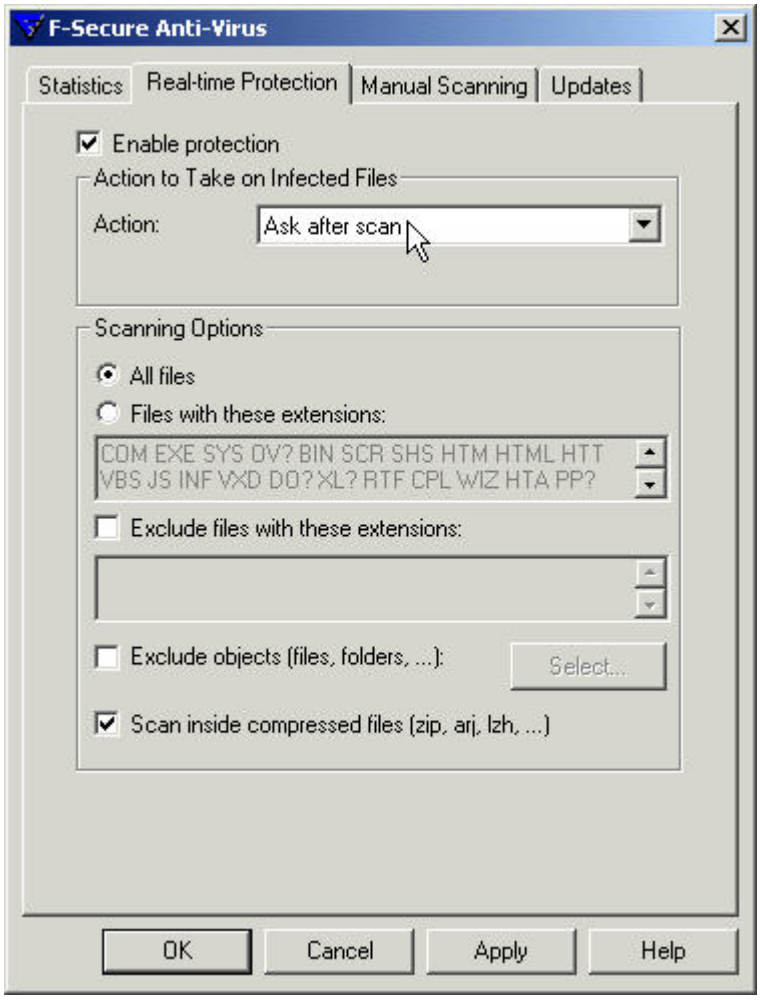

Figure 10-7. F-Secure Anti-Virus Real-time Options Window

Once the options window is open, click on the **Real-time Protection** tab and ensure that the **Enable protection** checkbox is checked. In the **Scanning Options** section, it is recommended that the user check the **All files** radio button instead of the default **Files with these extensions** radio button. Once these settings are applied, real-time protection will be configured.

To configure the update settings manually for F-Secure, click on the Update tab on the same options window. The default settings for these options are acceptable with the exception of the **Remind me of updates setting**. As shown in Figure 10-8, this setting is set to 3 days instead of the default 7 days.

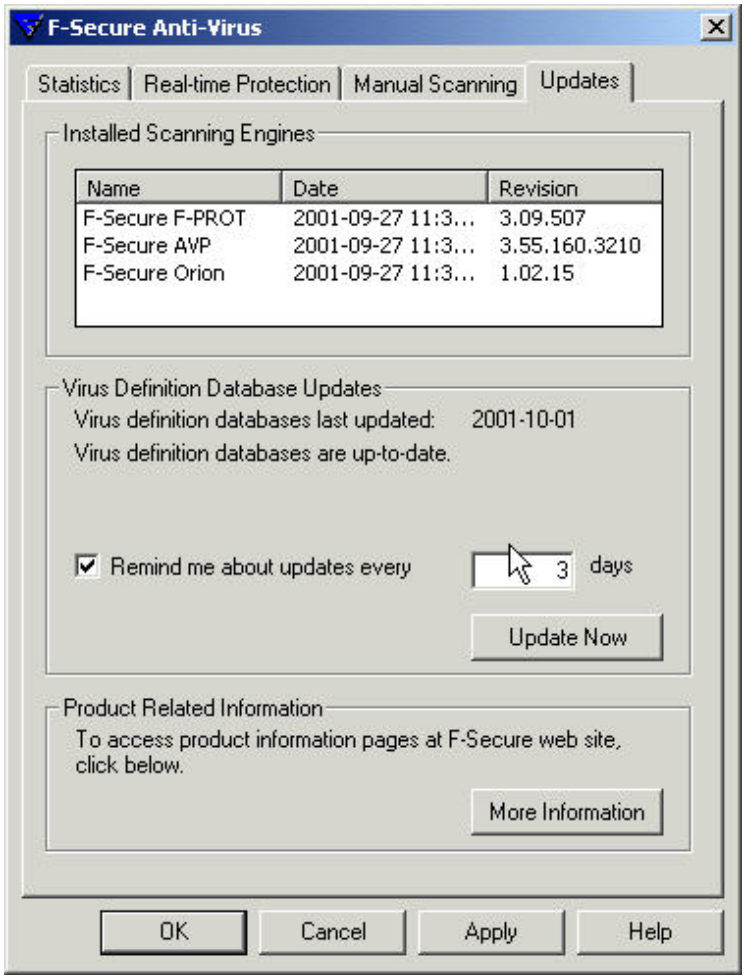

Figure 10-8. F-Secure Anti-Virus Update Options Window

10.2 E-mail Clients

There is no question of the importance of e-mail communications in today's marketplace. Unfortunately, e-mail is one of the primary mediums of distributing malicious code. Securing e-mail applications involves setting up virus scanners to scan all incoming messages, raising user awareness, and properly configuring e-mail clients. This section focuses on the proper configuration of two popular e-mail applications: Microsoft Outlook and Eudora. To operate an e-mail application in a secure manner, it is recommended that the user patch the software regularly, restrict the execution of active code, and understand the implication of opening an attachment.

10.2.1 Microsoft Outlook Security

The primary method of maintaining the security of Microsoft Outlook is to ensure that all necessary patches and hotfixes are promptly applied. Microsoft Outlook patches can be found at the Microsoft Office update Web site:
|http://office.microsoft.com/productupdates

Visit the update site often and consider applying all of the patches recommended, as long as there are no system or network conflicts. The Microsoft Office update site is discussed in detail in Section 10.4, Productivity Applications.

Note: Microsoft Outlook shares many components with the Internet Explorer Web browser. This means that the ability to install a Microsoft Outlook patch is dependent on which version of IE is installed. Ensure that the latest stable version of IE is available before visiting the Office Update Web site.

10.2.1.1 Microsoft Visual Basic Scripting. Microsoft launched itself into the modern scripting world with the release of Visual Basic Script (VBS). VBS, combined with other Windows 2000 utilities, enables a user to automate many of the management and repetitive tasks on the Windows 2000 Professional OS. Because of VBS's powerful interoperability features, it has become a delivery mechanism for worms and viruses on the Microsoft Windows platform. A VBS worm can propagate itself by dynamically accessing a user's address book and sending an infected message to every recipient.

Intelligent worms have been developed that include programming logic to generate random and very enticing subject lines. The entire Internet world moves at such breakneck speed today that it is dangerously easy to open a message with a subject that says "Here is the file you requested" without looking at the sender. These intelligent worms can rapidly spread throughout an enterprise or even the entire Internet as a result of the default interoperability of the Windows 2000 Professional and MS Office.

The following paragraphs focus on the protection of the enterprise and workgroup networks by disabling features that leave Outlook susceptible to malicious code. The recommended method o disabling VBS-driven malicious code is to follow the steps listed below:

1. Follow these steps to remove VBS from associated file types.
    a. Open **My Computer** window.
    b. Click on **Tools** menu options, and click on **Folder Options** menu choice.
    c. Click on the **File Types** tab to display a list of known file types for Windows 2000 Professional, as shown in Figure 10-9.
    d. Find and delete all options associated in any way with VBS. File extensions usually include **.vbs** and **.vbe**. These associations can be reinserted at a later date if necessary. This step prevents VBS malicious code from being treated as an executable by Windows 2000 Professional, an important step to curbing malicious code propagation.

    Note: Removing VBS from the associated file types list can have an adverse effect on a system because of the automation capabilities that the Windows Scripting Host (WSH) and VBS provide. Be aware of this effect before removing these associations.

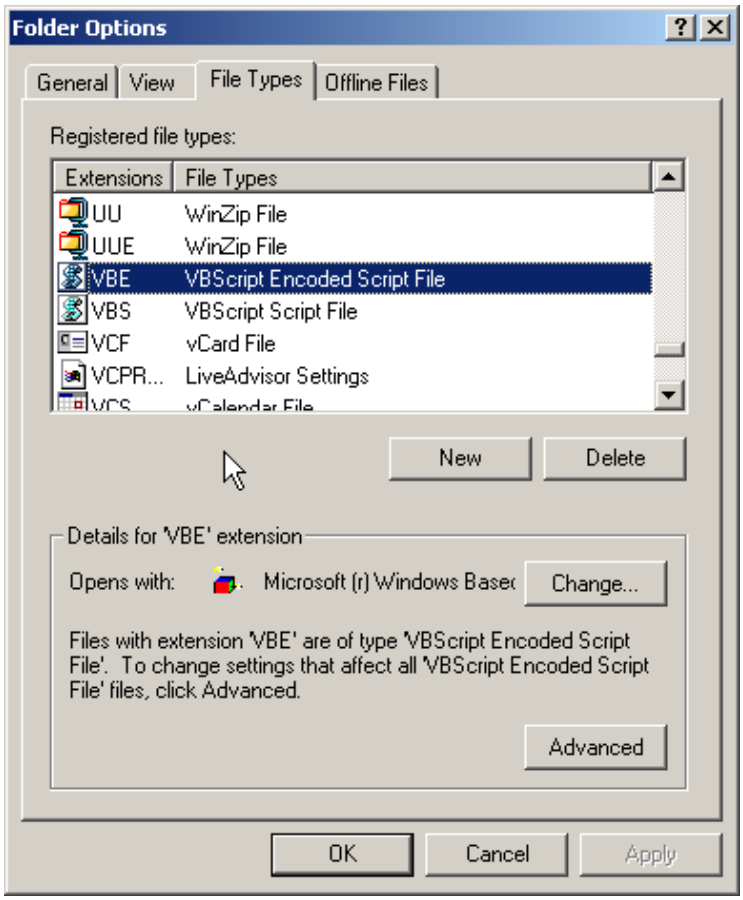

Figure 10-9. Windows 2000 Known File Types Window

2. The following steps describe how to change settings that open next unread message after moving or deleting a message.
    a. Click on the Microsoft Outlook **Tools** menu.
    b. Click on the **Options** menu choice.
    c. On the **Preferences** tab, click the **E-Mail Options** button, as shown in Figure 10-10.
    d. Under the **Message Handling** section, click the dropdown box next to **After moving or deleting an open item** and change the setting to read **Return to the Inbox.**
    e. Click the **OK** button to close the **E-Mail Options** window and return to Outlook.

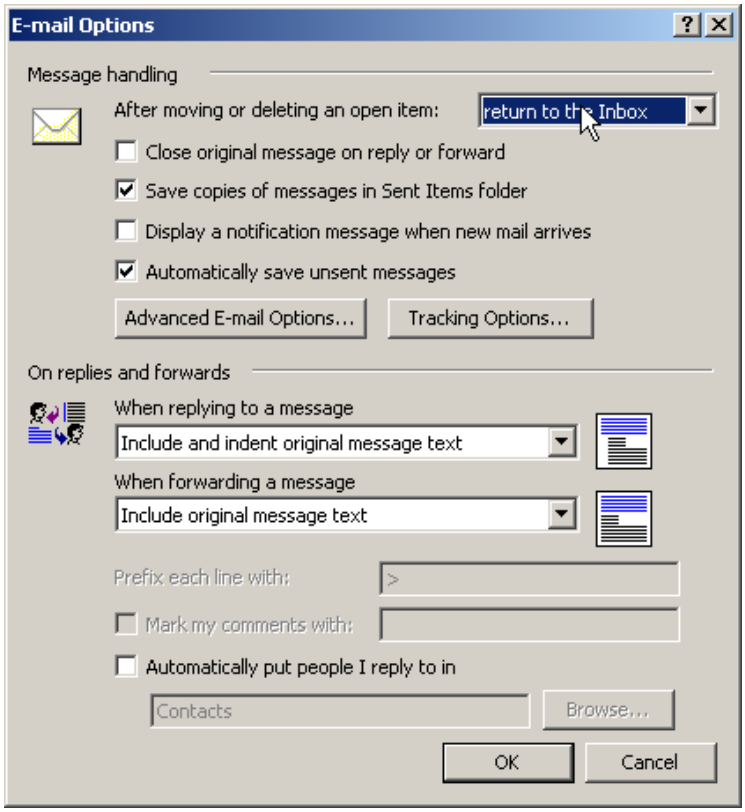

Figure 10-10. Change Behavior of Outlook after Interacting with New Message

3. Turning off the Outlook preview pane helps to prevent corrupt messages from executing their payload as soon as the message is selected.
    a. Click on the Microsoft Outlook **View** menu option.
    b. In the drop-down menu, locate the **Preview Pane** and **Auto Preview** menu option.
    c. If either or both of these are engaged, the icon next to their label will be depressed. If depressed, click the icon to disengage. Do this for both options.
    d. Third-party applications can be installed to preview e-mail messages in Microsoft Outlook, but this is beyond the scope of discussion.

    Note: Step 3 works in tandem with Step 2 to help disable malicious code execution when Outlook previews an infected message.

4. By default, Windows hides file extensions for known file types. Because **.vbs** is a known file type, the worm **ANNAKOURNIKOVA.JPEG.VBS** would be displayed as **ANNAKOURNIKOVA.JPEG**. This is a potentially dangerous situation. It is beneficial to have this displayed with the **.VBS** extension; therefore, we recognize it for what it really is a visual basic script, not an image file. Follow these steps to display all file extensions.
    a. Open the **Folder** Options window as in step 1.
    b. Click on the **View** tab.
    c. Find the checkbox that says **Hide file extensions for known file types** and verify that it is not checked as shown in Figure 10-11.

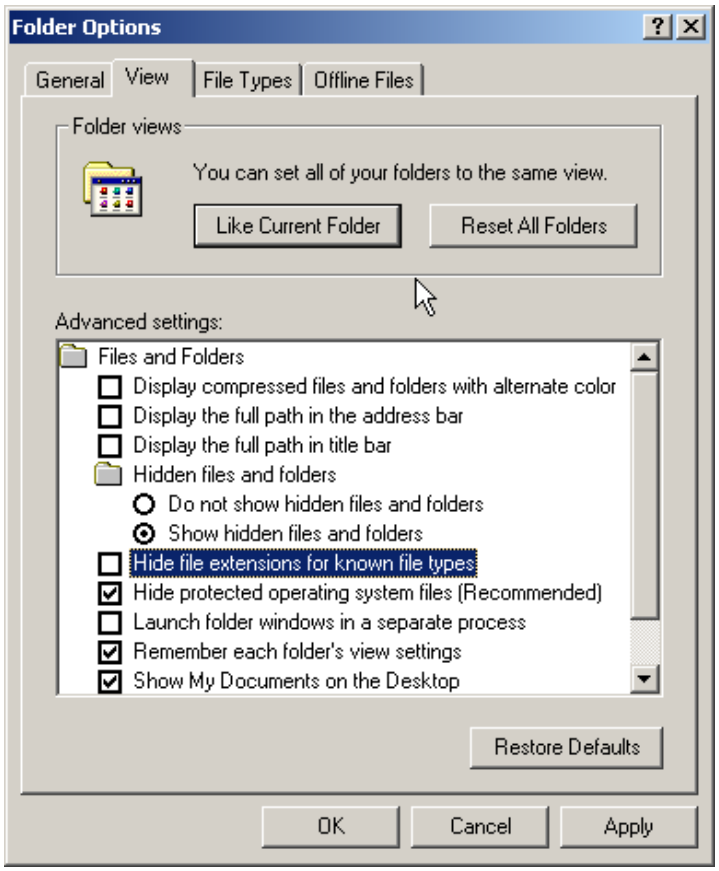

Figure 10-11. Set Windows 2000 to Display All Known File Extensions

10.2.1.2 Outlook Attachment Security. Outlook's attachment security setting determines what to do with executable attachments. The recommended value for this setting is **High**. Follow these steps to set the Outlook attachment security to **High**.

1. Start Microsoft Outlook and open the **Options** window from the **Tools** menu.
2. Select the **Security** tab and click on the **Attachment Security** button within the **Secure Content** section
3. In the Attachment Security window as shown in Figure 10-12, ensure that this setting is set on **High** Security and close the window.

Figure 10-12. Set Outlook Attachment Security to High

Also on the security **Options** tab, it is are recommended that users set the security **Zone** that Outlook will run under to **Restricted Sites**, as shown in Figure 10-13. Zone security is discussed in Section 10.3.1, Internet Explorer.

Note: The **attachment security option may not be available** if all current hotfixes have been applied to Outlook 2000. This is a known problem that Microsoft has resolved; please refer to: http://support.microsoft.com/default.aspx?scid=kb;EN-US;q277704.

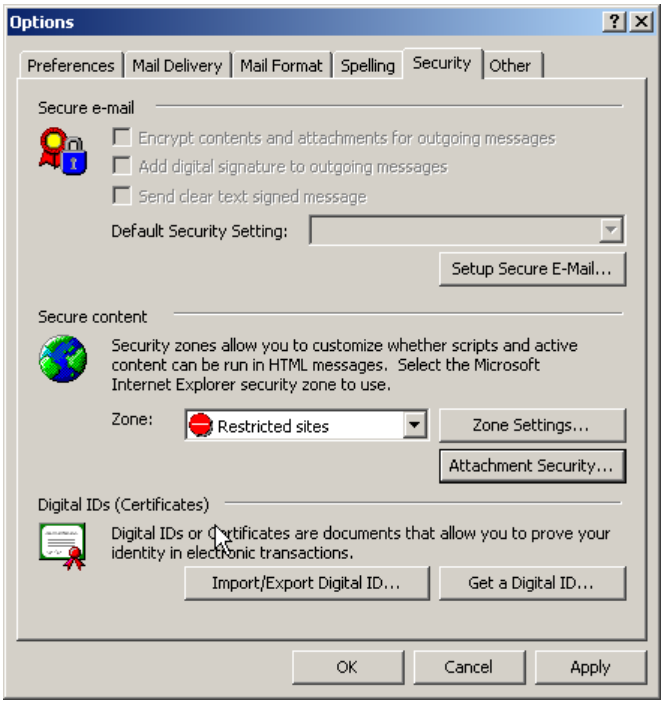

Figure 10-13. Set Outlook Security Zone

It is also recommended that users set the **Macro Security level** for Outlook to **High** as with all other Microsoft Office products. Follow these steps to set the Macro security level.

1. Expand the **Macro** submenu from the **Tools** menu option and select the **Security** choice. Set the **Security Level** to **High**, as shown in
2. Figure 10-14.

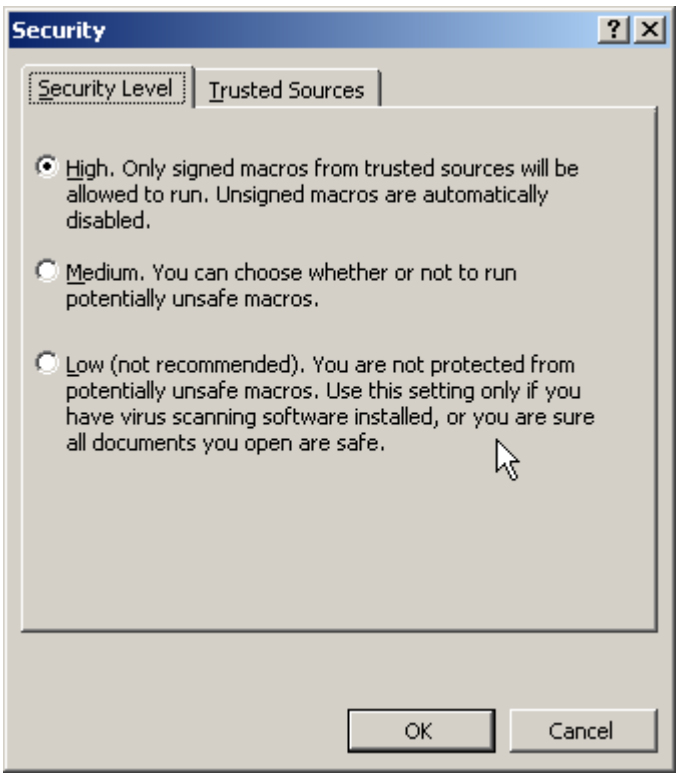

Figure 10-14. Set Outlook Macro Security

10.2.2 Qualcomm Eudora

The current version of Eudora is 5.1, developed by Qualcomm. Although not as integrated with other products, or parts of Windows 2000 as Microsoft Outlook, many of the steps described above to secure Microsoft Outlook also apply to securing Eudora. The notion of updating software should be extended to any installed on a system. It is important to check the Eudora Web site for the latest updates available: http://www.eudora.com/

Malicious active content transmitted via e-mail messages is also a concern to Eudora. Just as Microsoft Outlook does, Eudora can warn a user about interacting with a file based on the file extension. Eudora is configured to alert users with a dialog box when they are about to open a file with a registered file extension that is on Eudora's WarnLaunchExtensions list. This list deals with active content types, trying to prevent users from executing a program that they have downloaded from a potentially infected e-mail message. This list is configured in the Eudora.ini properties file, which is installed where the Eudora inbox files are stored. Figure 10-15 shows an example of **Eudora.ini**.

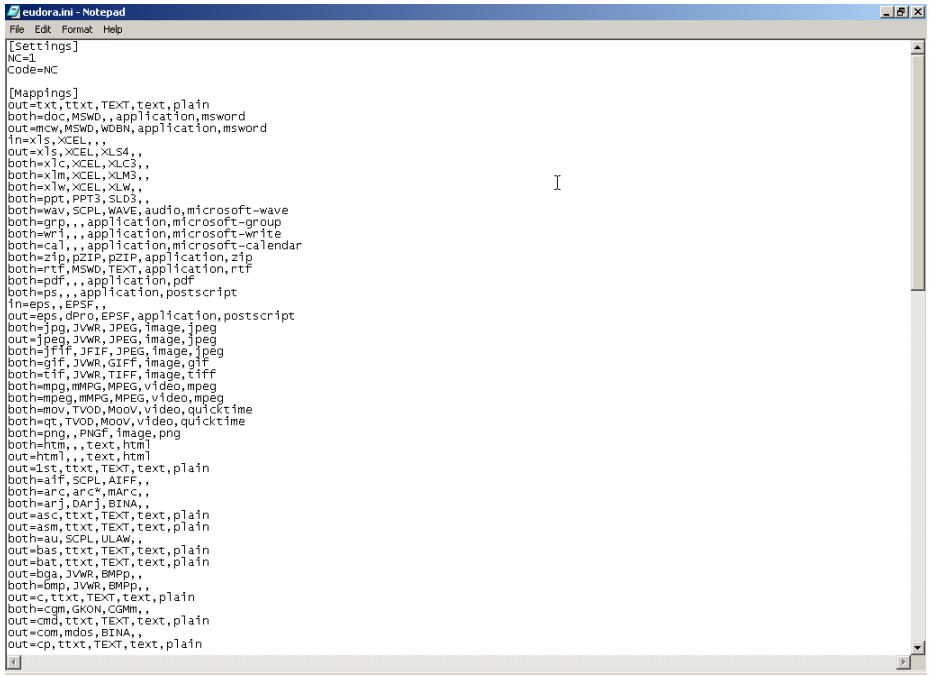

Figure 10-15. Eudora.ini Properties File

During the installation of Eudora, the user must select the location to install user data files including **Eudora.ini**, as shown in Figure 10-16.

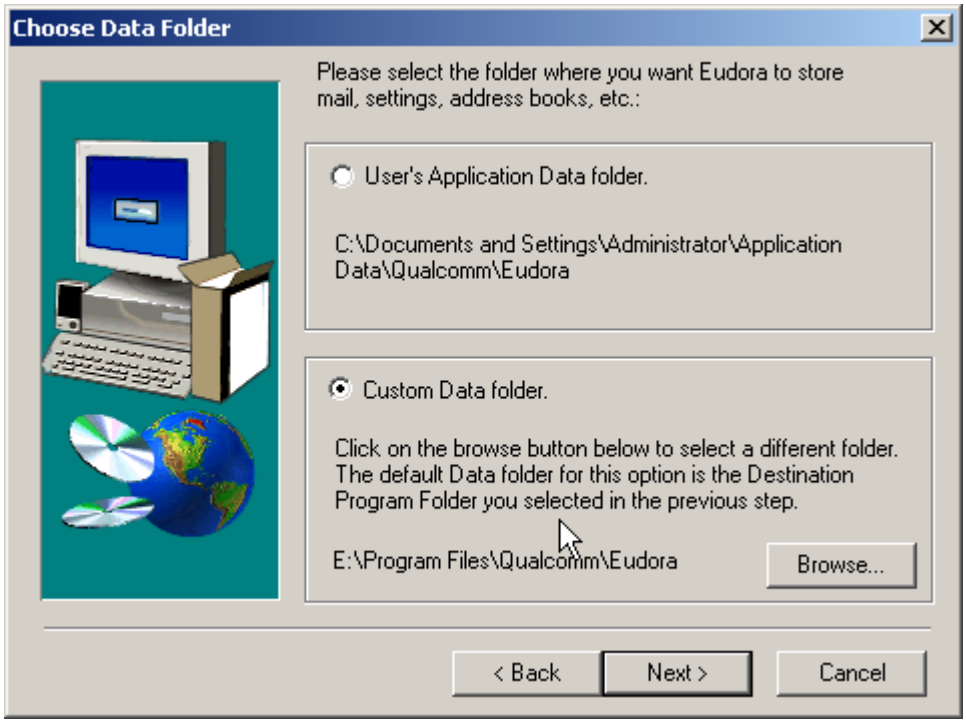

Figure 10-16. Choose Where to Install Eudora Data Files

This is a critical step in the installation process. Here, this user has chosen to install the data files into the same directory in which the Eudora program was chosen to install. This decision can create a potentially dangerous situation because of the permissions of this directory. The directory in which Eudora is installed is configured by default to give the **Everyone** group full control over the directory, as shown in Figure 10-17.

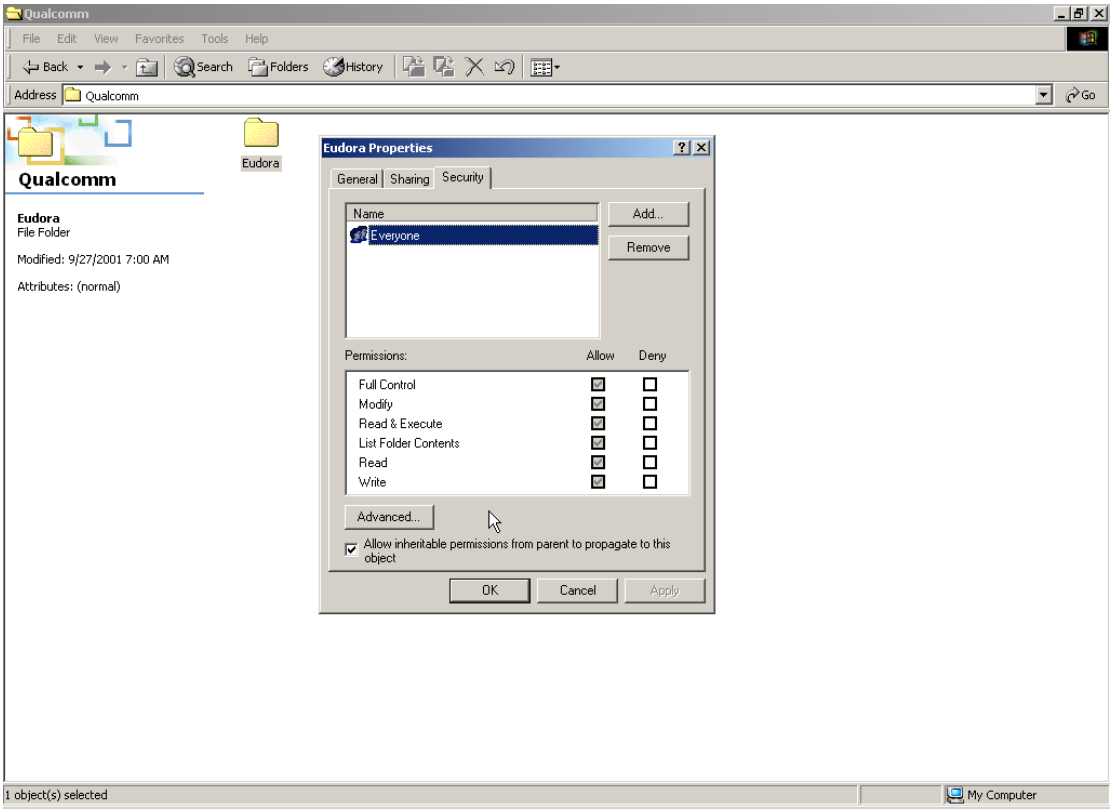

Figure 10-17. Eudora Default Directory Permissions

In this example, parent permissions are set to propagate to children elements—that is, the **Eudora.ini** file. The message data files for this Eudora user are accessible by anyone with access to the machine. To prevent this action from occurring during the installation process, install all Eudora data files into a user's application data directory for Windows 2000 Professional because this directory is already configured correctly.

When Eudora is first executed, additional settings should be modified to increase security. Similar to Microsoft Outlook, it is recommended that Eudora's abilities to interact with other executables be minimized. To disable Eudora from interpreting Active Content in this manner, perform the following steps:

1. Start **Eudora**.
2. Edit Eudora options.
    a. Click on the **Tools** menu option.
    b. Click on the **Options** menu choice to open the Edit Options window.
3. Open Viewing Mail Option/Disallow Executables in HTML content.
    a. In the scrolling list on the left side of the window, find the **Viewing Mail** option and click on it.
    b. Ensure that the bottom checkbox **Allow executables in HTML content is not checked,** as shown in Figure 10-18.
    c. Deselect the **Use Microsoft's viewer** checkbox.
    d. Deselect the **Automatically open next message** checkbox.

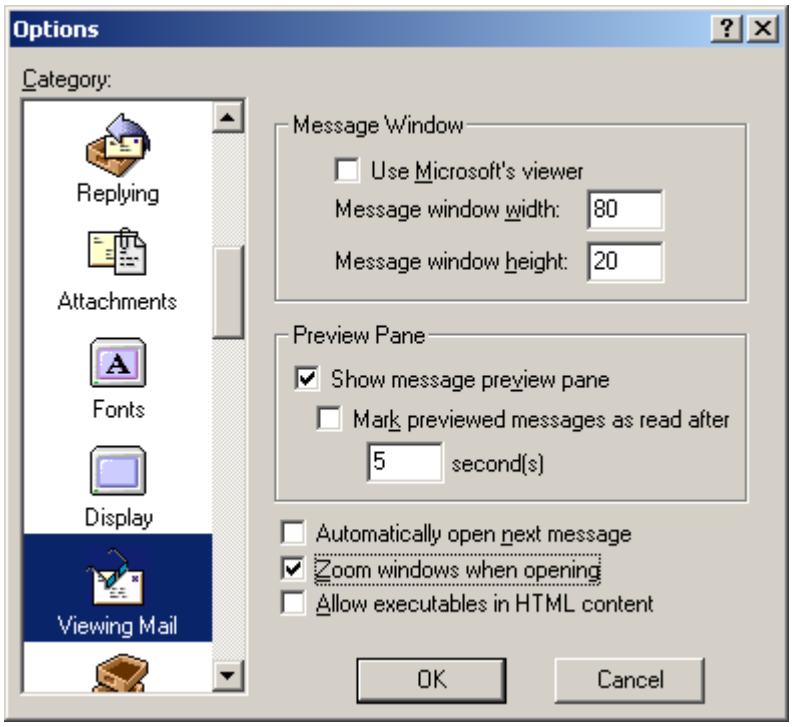

Figure 10-18. Disable Executables in HTML Messages in Eudora

4. Open Extra Warnings Options/Enable warnings for launching external programs.
    a. In the scrolling list on the left side of the window, find the Extra Warnings choice and click on it to open the **Extra Warnings** options.
    b. Ensure that the bottom two checkboxes, **Launch a program from a message** and **Launch a program externally**, are checked as shown in
    c. Figure 10-19.

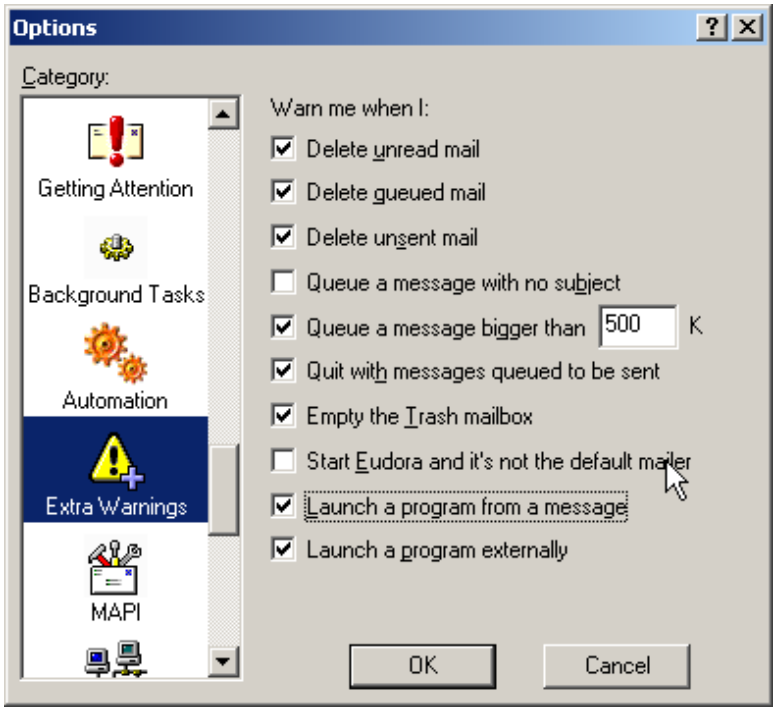

Figure 10-19. Enable Executable Warnings in Eudora

10.3 Web Browsers

The following sections discuss how to secure two popular Web browsers: Microsoft Internet Explorer and Netscape Navigator. Since Web browsers are capable of parsing active code in the form of JavaScript, Plug-ins, ActiveX, and Java, it is recommended that the user understands the implication of enabling these functions.

10.3.1 Microsoft Internet Explorer

Internet Explorer (IE) 5.01 is installed on Windows 2000 Professional by default. Every Windows 2000 Professional should ensure stability of newer versions of IE before upgrading. Internet Explorer interacts with numerous components within the Windows 2000 OS most notably the Windows Explorer, **explorer.exe**. Upgrades and patches are continually available for IE; it is imperative to test and install new patches regularly. The Microsoft Internet Explorer home page is the best place for additional information on IE. The Microsoft homepage for IE is http://www.microsoft.com/windows/ie.

Internet Explorer uses a capabilities/trust model, called Zone Security, which was introduced in version 4.x of IE. In this model Web sites are permitted to perform certain actions based on their locale. Possible locales are Internet, Local Intranet, Trusted Sites, and Restricted Sites. Each site can be set to allow certain actions. The possible security levels are High, Medium, Medium-Low, and Low. Users can modify the security level for each zone, but IE will warn them if they exceed the recommended security level.

The process of upgrading IE is simple; it involves a visit to the Windows Update site discussed in Section 7. From this site, users can choose to install a service pack to their existing version of IE or to download the Internet Explorer update program.

One recommendation for Domestic US users, which is independent of the version of IE, is to upgrade the encryption level to 128 bits; Windows 2000 SP2 and higher provides 128 bits encryption as a default. It is recommended that the most current service pack be installed. If the service pack cannot be installed, the Windows 2000 Professional high-encryption pack can be downloaded from the Windows Update site. It is recommended that users enable active content within Internet Explorer when needed. Disabling the active content will disable the functionality of many Web services. The Computer Emergency Response Team (CERT) and the SysAdmin, Audit, Network, Security (SANS) Institute are among the organizations that advocate selectively or completely disabling Active Content. This means that all scripting languages such as JavaScript or Jscript, VB Script, and ActiveX will be disabled. If your site security requirements require this security measure, perform the following steps to disable Active Content in IE:

1. Open the **Internet Options** from the **Tools** menu choice.
2. Click on the **Security** tab, and click on the **Custom Level** button near the bottom of the window.
   Note: Because you can customize the security settings for each possible zone, be sure that the Internet Zone is highlighted before clicking on the Custom Level button.
3. Scroll down to the setting labeled **Script ActiveX controls marked safe for scripting** in the **Security Settings** dialog box; then, check the **Disable** option.
   Note: By changing this setting only, ActiveX controls are effectively disabled and no warning messages are displayed if a page attempts to use an ActiveX control.
4. Find the **Scripting** section of options in the scroll list. This option is the second to last major section of options.
5. Check the **Disable** button for the **Active Scripting** choice as shown in Figure 10-20.
   Note: Changing only this setting disables all scripting languages, including ActiveX.

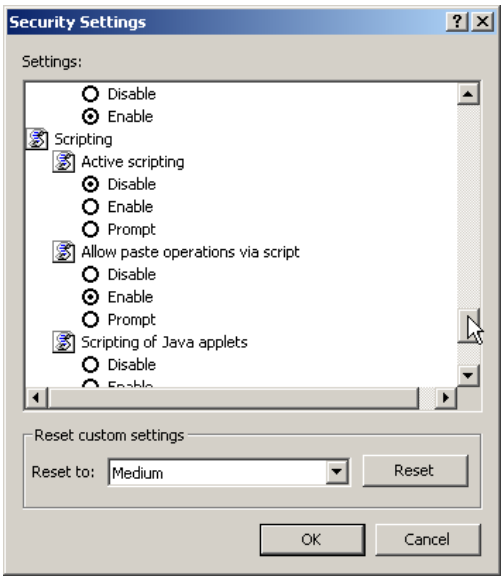

Figure 10-20. Disable Scripting in Internet Explorer

It is recommended that Java be enabled within Internet Explorer only when needed. Follow these steps to configure the Java option.

1. Open the same Custom Levels Security window for the Internet zone as in the previous example.
2. Scroll to the **Microsoft VM** section.
3. To disable Java, click on the **Disable Java** option as shown in Figure 10-21.

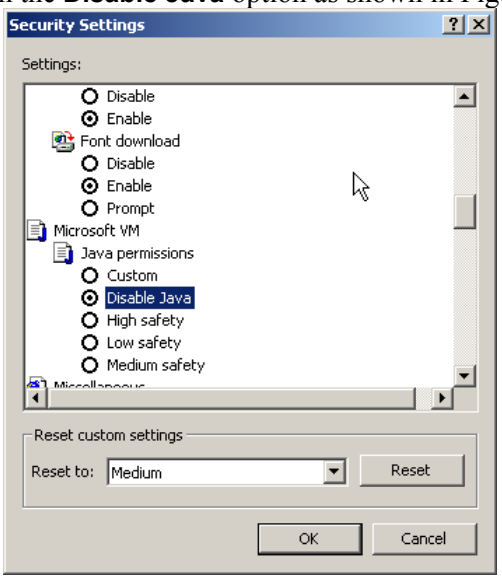

Figure 10-21. Disable Java in Internet Explorer

Note: Internet Explorer allows customizations of Java virtual machine (JVM) permissions by clicking on the **Custom** radio button under the **Java Permissions**. This action enables a **Java Custom Setting** button at the bottom of the window providing granular controls over the Java functions as shown in Figure 10-22. Discussions about the specific settings within the advanced window are beyond the scope of this document.

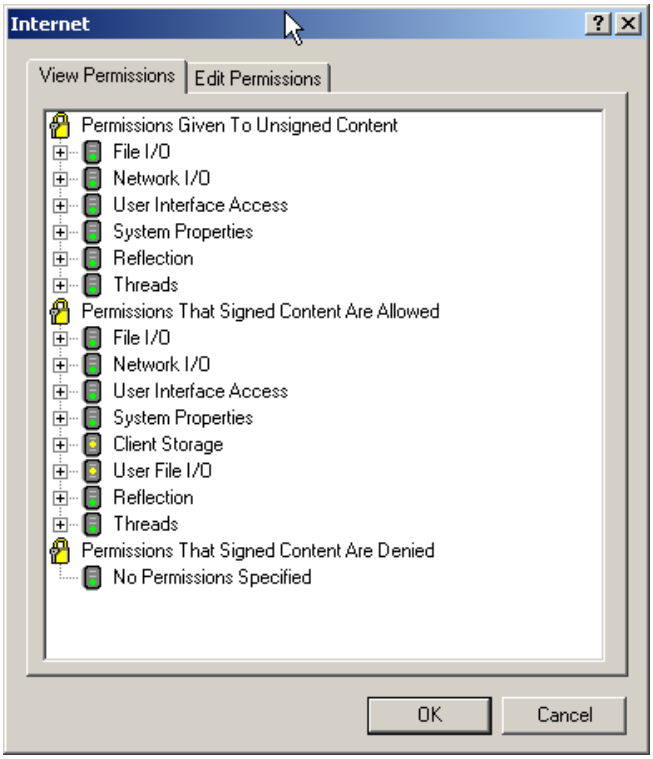

Figure 10-22. Set Custom Microsoft JVM Permissions

In terms of user privacy, the cache files collected by IE should be emptied after every Web session, unless the environment warrants their usage. A low-bandwidth Internet connection may provide value in the use of the cache for performance reasons, yet in most other cases users should take steps to ensure their Internet browsing privacy is kept secure.

To empty the cache for IE perform the following steps:

1. Open the **Internet Options** window from the Tools menu.
2. Ensure that the **General** tab is selected. In the middle of the window where it says **Temporary Internet files**, click the **Delete Files** button.
3. In the confirmation dialog box that appears, click the **OK** button to continue as shown in Figure 10-23.

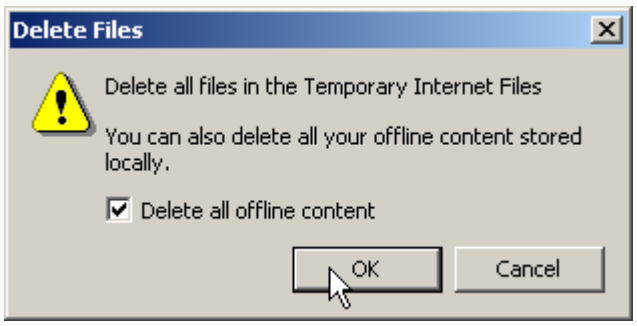

Figure 10-23. Confirm Clearing Cache on Internet Explorer

Note: A user can delete all Web content downloaded from IE by checking the "Delete all offline content" box as well.

Finally, note that Microsoft has provided a tool to customize IE for a moderate to large-size organization with these types of settings already configured. The Internet Explorer Administrators Kit (IEAK) can be obtained from the Microsoft URL:
http://www.microsoft.com/windows/ieak/default.asp

10.3.2 Netscape Navigator

Netscape Navigator is a part of the larger Netscape Communicator package. Although the component that browses and renders Internet content is called the Netscape Navigator (current version is 4.08), this discussion focuses on the entire Netscape Communicator package version 4.79. Netscape also offers the Communicator package in varying encryption strengths; it is recommended that qualified users download the 128-bit version. The Netscape Communicator package can be downloaded from the Netscape Web site at the following URL:
http://home.netscape.com/computing/download/index.html?cp=hophb2

This Web page will examine the JavaScript User Agent string within the registry to determine which browser users have installed and whether a newer version is available. To skip this automated process and proceed directly to downloading Netscape Communicator, users should visit the following URL:
http://home.netscape.com/download/1126101/10000-----_qual.html?cp=dowcomm

This URL starts users on a process of determining which type of installation of Netscape Communicator they wish to download. The only concern is the choice of installing Netscape Communicator with or without the SmartDownload file download manager utility. Users should not install SmartDownload if they wish to have full control over their file downloads.

The SmartDownload utility was first introduced in Netscape Navigator versions 3.x and Communicator/Navigator versions 4.x. SmartDownload version 1.3 and later will also work with Internet Explorer version 4.x and above. Users must be aware that installing SmartDownload means that the SmartDownload utility will control any file that is downloaded from the Internet using FTP or Hypertext Transfer Protocol (HTTP). If users decide they wish to use SmartDownload, they can download the SmartDownload utility from Netscape by itself from the following URL:
http://home.netscape.com/download/smartdownload.html?cp=dowdep6

A user with Administrative privileges must perform the installation of Netscape because the installation process attempts to read values from the registry. Figure 10-24 shows the error message that is displayed when the Netscape installation cannot successfully access the registry.

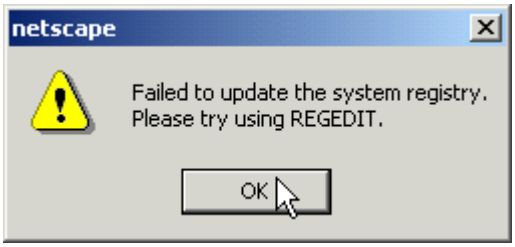

Figure 10-24. Registry Error Installing Netscape as a Regular User

Table 10-1 lists the registry keys that Netscape attempts to unsuccessfully access when running the installation process as a regular user.

Table 10-1. Registry Keys Netscape Cannot Successfully Access During Installation

HKLM\System\CurrentControlSet\Control\MediaProperties\PrivateProperties\Joystick\Winmm
HKLM\System\CurrentControlSet\Control\MediaProperties\PrivateProperties\Joystick\Winmm
HKLM\SOFTWARE\Netscape\Netscape Navigator\Users\
HKCR\CLSID\{481ED670-9D30-11ce-8F9B-0800091AC64E
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\netscape.exe
HKCR\Netscape.TalkNav.1\CLSID
HKCR\Netscape.Registry.1\CLSID
HKCR\Netscape.Help.1\CLSID
HKCR\Netscape.Network.1\CLSID
HKCR\NetscapeMarkup\CLSID
HKCR\CLSID\{61D8DE20-CA9A-11CE-9EA5-0080C82BE3B6}\ProgID

Users who download and install Netscape Communicator may not wish to have America Online (AOL) Instant Messenger installed with Communicator. Netscape provides unsupported instructions for how to remove AOL Instant Messenger from a system at the following URL:
http://help.netscape.com/kb/consumer/19971116-8.html

Note: Enable the AOL Instant Messenger only if required.

Similar to Internet Explorer, Netscape users must check regularly for updates to Netscape Communicator. These updates, which are published in the form of a new release of the Communicator package, often include enhancements to current features and new features, but more importantly, fixes to security vulnerabilities that are discovered. Two methods exist for updating and upgrading Netscape:

- Visiting the URLs noted above, these Web pages will automatically determine which version of Netscape is installed and if a new version is available.
- Using SmartUpdate manager will determine if any updates are available.

Users must be aware that using the SmartUpdate manager to update Netscape involves Java applets and granting explicit Java permissions, cookies, and JavaScript enabled. This can interfere with organizations

that have existing rules regarding the presence of Active Content. Usage of the SmartUpdate manager is a four-step process:

- Choosing software updates
- Reviewing chosen updates
- Signing into Netscape Net Center
- Downloading updates and installing locally.

When installing software updates, users are presented with a dialog box requesting Java permissions, as shown in Figure 10-25. This dialog box recognizes a digitally signed Java applet. Netscape forces developers to sign applets based on permissions. Users are permitted to permit or deny any action they choose.

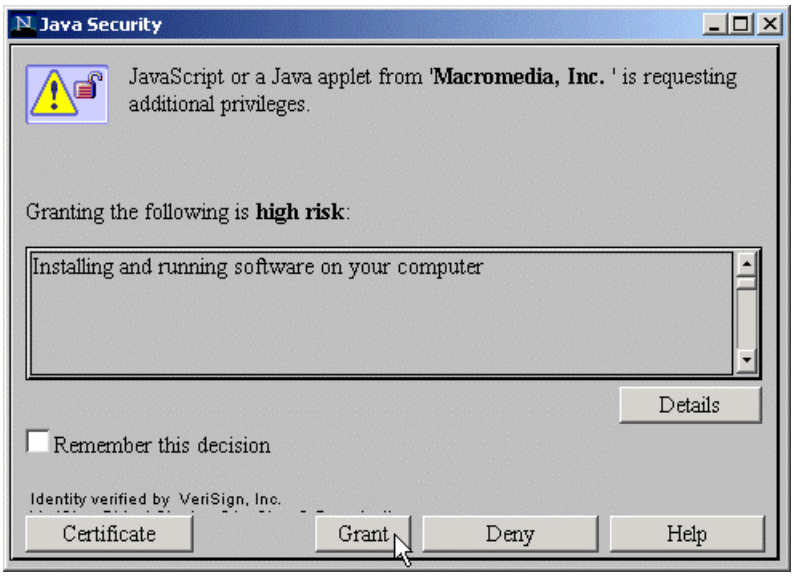

Figure 10-25. Netscape Communicator Update Requesting Java Permission

Users should not grant this software the permission to install unless they can be sure of the integrity of what they are installing. To prevent software from installing, press the **Deny** button shown in Figure 10-25.

Netscape has attempted to unify the configuration data for Netscape Communicator from platform to platform and user to user by storing configuration information in the file **nsreg.dat**. This file is stored in the **%SystemRoot%** folder by default. Default directory permissions prevent Netscape from modifying this file after installation. To enable Netscape to modify this file, it must allow the **Everyone** group read/write permission within its ACL.

Netscape allows users to examine any Web page for its security-related information, including the presence of signed applets. Pressing the **Security** button on the Netscape toolbar will open the **Security Information** window for that particular page. Figure 10-26 shows an example of the Signed **Java/JavaScript** window. If a Web page contains a signed applet, this window will show the information about the applet itself, including its code-signing certificate.

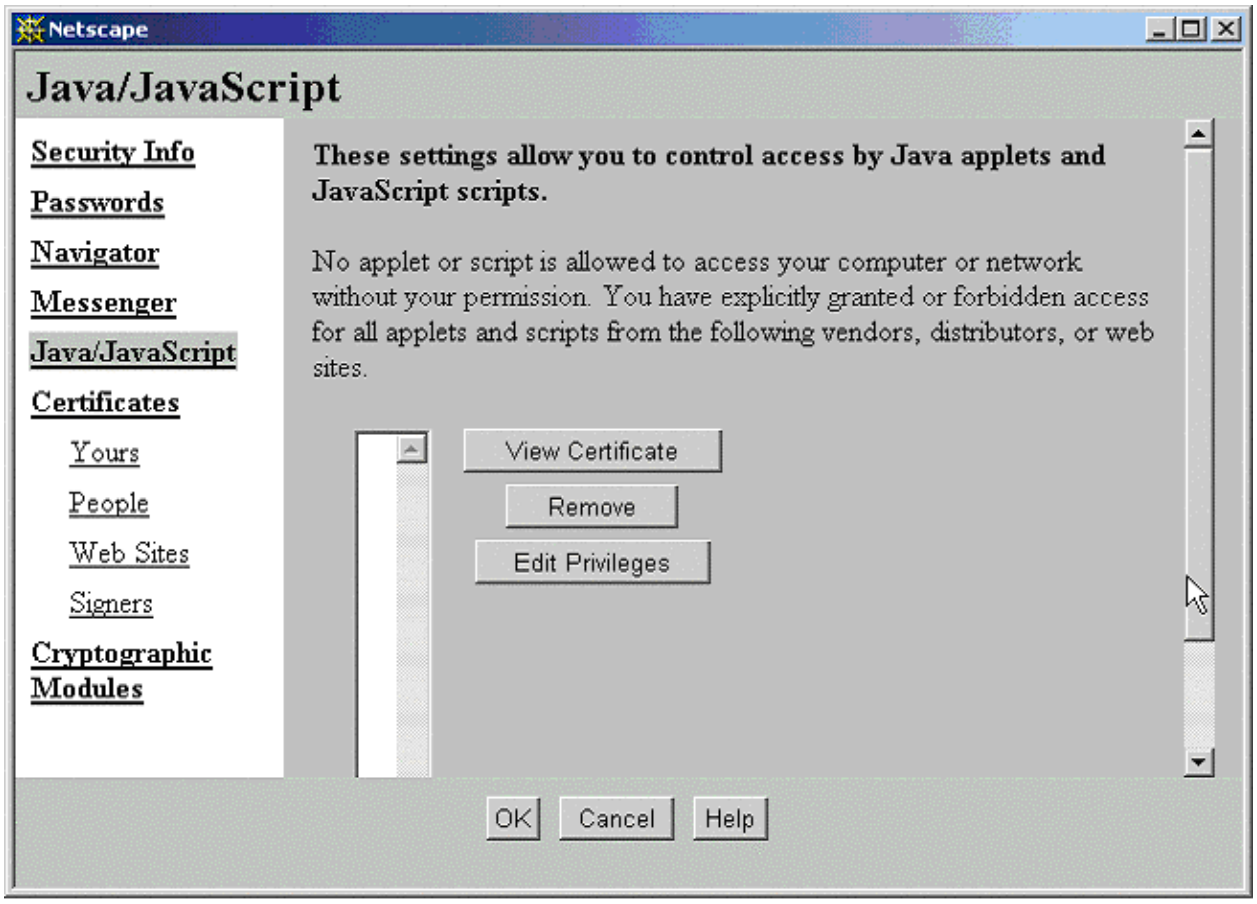

Figure 10-26. Netscape Signed Java Applet/JavaScript Window

Users who wish to disable Active Content technologies such as Java and JavaScript can do so by selecting **Preferences** found in the **Edit** menu. Under the **Advanced** option on the preferences window, users can selectively set **Enable Java** and **Enable JavaScript** options as shown in Figure 10-27. Users should not disable these technologies unless they are directed to do so by an SA or unless they are aware of the ramifications. As an example, users are prevented from updating Netscape with Active Content disabled.

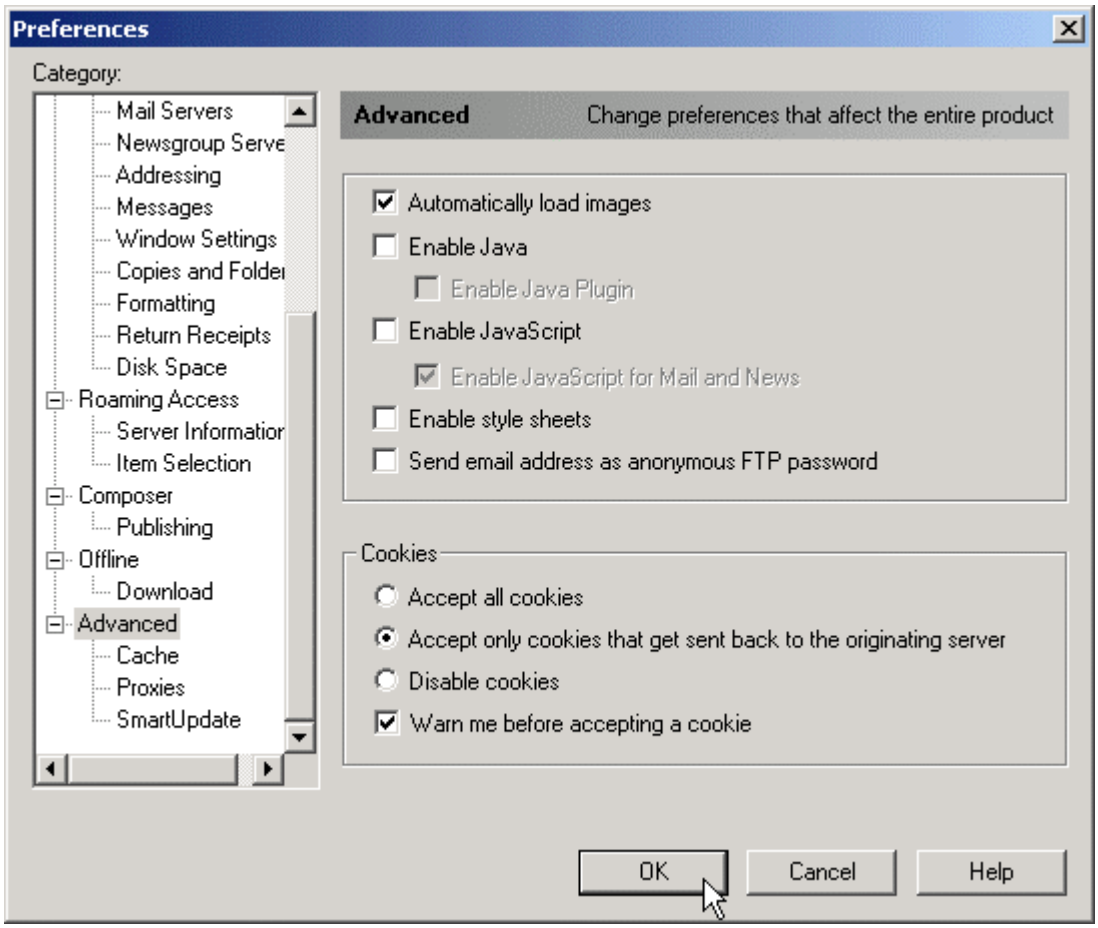

Figure 10-27. Disable Active Content within Netscape Communicator

Netscape differs from IE in the use of embedded content technologies such as ActiveX controls. Netscape uses embedded technology called plug-ins. Netscape cannot execute ActiveX controls without a third-party plugin. To list what plugins Netscape has installed, select the **About Plugins** options from the **Help** menu or type the following syntax at the Communicator Address bar:
about:plugins

This action will display a page similar to the example shown in Figure 10-28. This page, rendered by Netscape, lists information on all of the plug-ins currently installed.

It is recommended that the plugins not being used or installed by the user be disabled by deleting the corresponding **dll** file from the Communicator Program plugins directory. For example, delete the file **NP32DSW.DLL** to disable Shockwave.

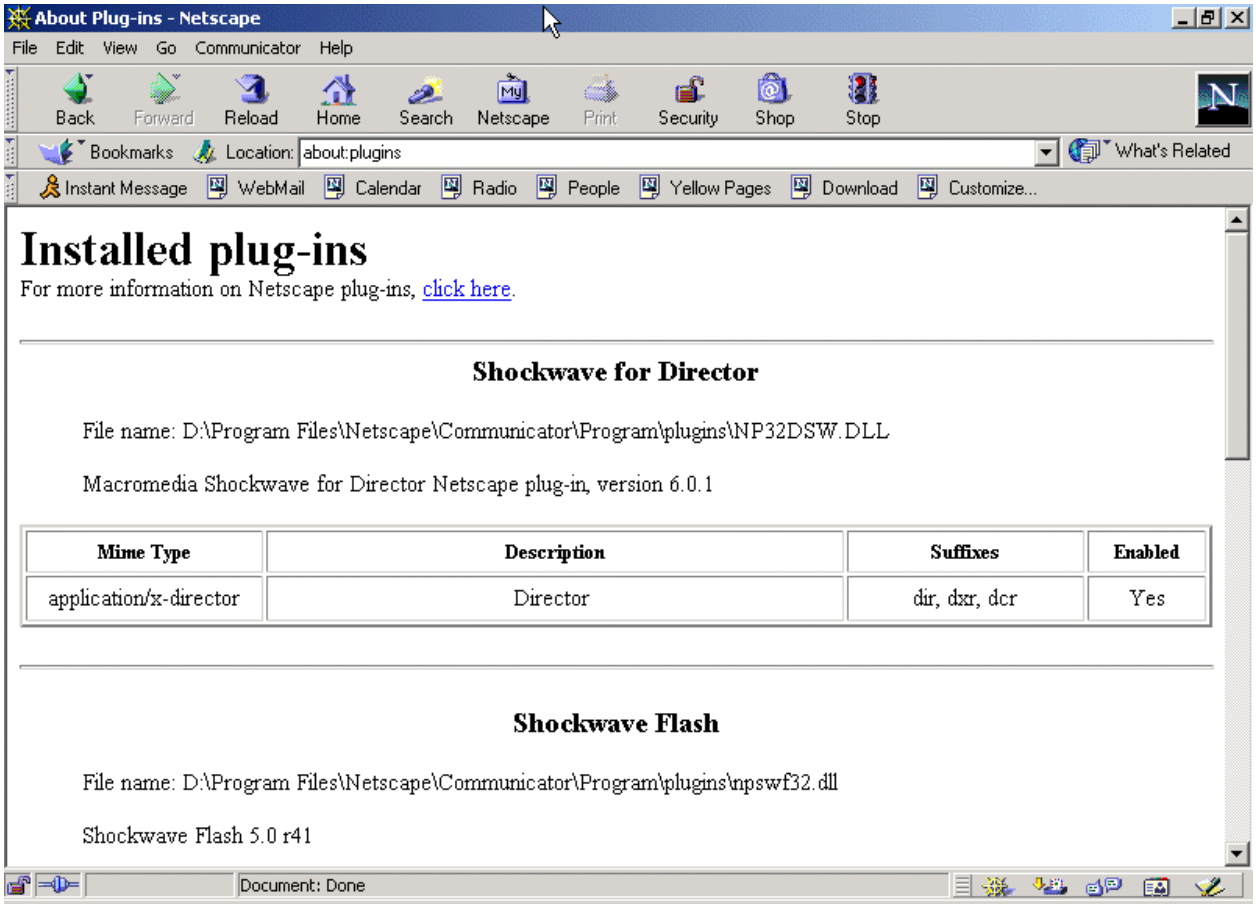

Figure 10-28. Installed Netscape Plugins

10.4 Productivity Applications

Productivity applications include the Microsoft Office Suite of applications. Microsoft Office is a series of interlocking applications using a significant amount of underlying shared code. The series of Office applications run on a specific dialect of Microsoft Visual Basic, called Visual Basic for Applications (VBA). These applications allow the use of macro scripting languages and imbedded URL tags. The macro security settings are set using macro security zones within Microsoft Office, the security settings for the imbedded URL tags are set within the Web browser; refer to Section 10.3. The Office applications seamlessly interoperate with each other and allow direct access to Web pages. Security must be configured for Web browsers and the Office applications to secure your system.

10.4.1 Microsoft Office Installation Issues

The Windows Installer for Microsoft Office 2000, shown in Figure 10-29, provides a simple interface to customize Microsoft Office 2000 installation. The custom installer allows rapid configuration of components to run from disk, run from CD, install on first use, or disable.

Note: Administrators should determine which component installation settings are required for their environment before the installation begins.

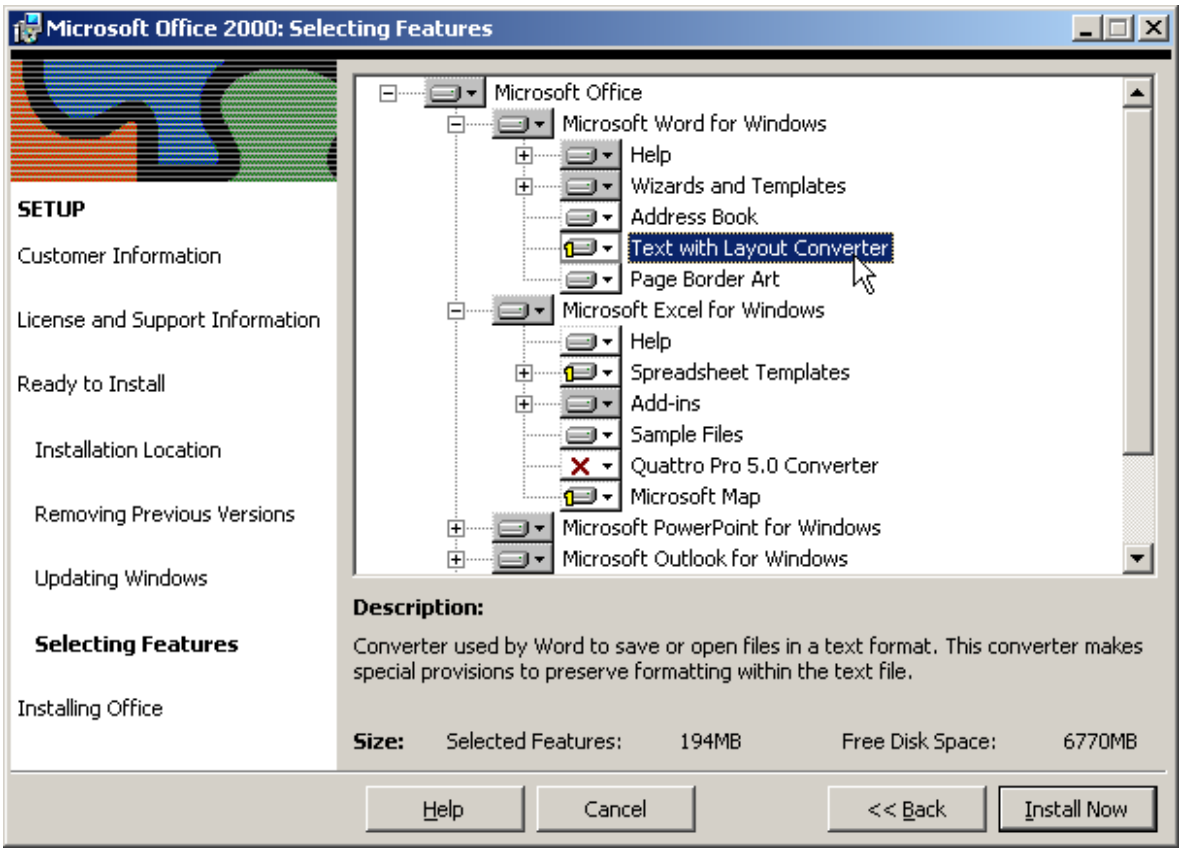

Figure 10-29. Office 2000 Installation Procedure

10.4.2 Microsoft Office Updates

As mentioned in Section 0, the method of obtaining and installing updates and patches to Microsoft Office titles is through the Office Update Web site located at http://office.microsoft.com/ProductUpdates/default.aspx

Note: This site requires the use of ActiveX scripting for correct operation. To get Office updates without ActiveX scripting enabled, use http://office.microsoft.com/Downloads/default.aspx to download and install the updates for your system.

Developing a habit of frequently visiting the update site is recommended. Microsoft uses Service Releases (SR) to perform Office updates. Although Office XP is commercially available, the current SR for Microsoft Office 2000 is SR-1.

Note: When deciding to install an SR, remember that SRs tend to be very large. Download and install the service pack SP2, and other post-SP2 patches to update Office 2000 SR-1.

10.4.3 Office 2000 Macro Virus Security

Office 2000 introduced digital signatures to help users distinguish legitimate code from undesirable and viral code. By using digital signatures for the Macros in use within your organization, users can be

reasonably sure of the origin of the Macro they are using. Office 2000 silently disables nonsigned macros when the Office 2000 Security Level feature is set to "High." The default security setting for Word 2000 is "High." By removing the chance that a user "accidentally" enables a virus-infected document, the high security level reduces the spread of macro viruses. If all legitimate macros are digitally signed, users will see a security warning only when a macro attempts to run with digital signature information. Otherwise, the macro will be disabled without information about the disabling sent to the user.

The following Office applications include security level and digital signature features for VBA macros: Word, Excel, and PowerPoint. To take advantage of the benefits of macro digital signatures, Office 2000 uses security levels. Medium security level provides the user with a choice to enable or disable the macros on a file-by-file basis. High security level allows only signed and trusted code to run. Low security level turns off all macro security warnings in Office. The security level can be set with the Security dialog in the Tools/Macro menu.

When opening a file with macros under medium security, a security warning offers the user a choice between enabling or disabling macros. The Office 2000 Medium Security Warning dialog has digital signature information, if it is available for the file being opened. This security level allows existing Office 97 solutions, which are not signed, to be enabled. Once a user chooses to trust all macros from a source, Office 2000 on medium security will automatically enable signed macros from that trusted source—without any security alerts.

Under high security, Office 2000 silently disables unsigned macros. This helps avoid accidental enabling of potentially dangerous macros when users carelessly dismiss the Security Warning dialog with the Enable Macros button. To help fight the larger number of Word macro viruses spread through documents, Word 2000 is set to high security level by default. Under high security, a security warning is shown for digitally signed macros that have not been previously added to the Trusted Sources list. This warning enables users to inspect the digital certificate; if they choose to trust all macros from the source, they may then choose to Enable Macros. The Enable Macros button is disabled until the user decides to check the Always trust macros from this source checkbox.

Note: Office 2000 allows installed add-ins and templates to be treated with the same security settings enforced during the opening of a document. The option is controlled by the **Trust all installed add-ins and templates** checkbox in the **Trusted Sources** tab of the Security dialog under the **Tools|Macro** menu. This checkbox is selected by default. Clearing the checkbox will cause the Office 2000 macro security settings to be applied to the installed add-ins.

NIST recommends that the High macro security setting be enabled for all Office applications. To verify that the Macro Security is set to **High**, execute MS Word and select **Tools | Macro | Security**.

Note: If completely disabling all Macros in Office applications is desired, the following registry settings will accomplish this task:

HKEY_Local_Machine\Software\Microsoft\Office\9.0\Excel\Security\Level=3

HKEY_Local_Machine\Software\Microsoft\Office\9.0\Word\Security\Level=3

HKEY_Local_Machine\Software\Microsoft\Office\9.0\PowerPoint\Security\Level=3

HKEY_Local_Machine\Software\Microsoft\Office\9.0\Outlook\Security\Level=3

HKEY_Local_Machine\Software\Microsoft\Office\9.0\Access\Security\Level=3

HKEY_Local_Machine\Software\Microsoft\Office\9.0\Excel\Security\DontTrustInstalledFiles=1

HKEY_Local_Machine\Software\Microsoft\Office\9.0\Word\Security\DontTrustInstalledFiles=1

HKEY_Local_Machine\Software\Microsoft\Office\9.0\PowerPoint\Security\DontTrustInstalledFiles=1

HKEY_Local_Machine\Software\Microsoft\Office\9.0\Outlook\Security\DontTrustInstalledFiles=1

HKEY_Local_Machine\Software\Microsoft\Office\9.0\Access\Security\DontTrustInstalledFiles=1

HKEY_Local_Machine\Software\Microsoft\VBA\Trusted\"No certificate will be trusted. - InfoServices"=hex:d3,0f,d6,00,91,21,bf,51,7e,60,48,a2,99,ba,25,00,b7,96,08,01

NSA has produced an excellent guide on executable content and countermeasures that applies specifically to Office 97. It is located at http://nsa1.www.conxion.com/emailexec/guides/eec-3.pdf

10.5 Summary of Recommendations

- Antivirus Scanners
  - Do not install competing Antivirus software on the same machine.
  - Ensure that Antivirus scanners are configured properly and updated weekly or as often as a new virus is discovered.
  - Periodically perform a full scan of your system.
  - Enable Auto-Protection scanning of new software and documents introduced to your system (all file types).
  - Enable e-mail and Internet scanning.
- E-mail Clients
  - Frequently update e-mail clients.
  - Disable VBS in Microsoft Outlook.
  - Turn off the Outlook preview pane.
  - Display extensions for attachments.
  - Set Outlook's attachment security to HIGH.
  - Set Outlook's Macro Security level to HIGH.
  - Secure the user's e-mail data directory.
  - Disable executables in HTML content in Eudora.
  - Deselect the Use Microsoft's viewer option in Eudora.
  - Enable message warnings in Eudora.
- Web Browsers
  - Frequently update Web browsers.
  - Upgrade encryption level to 128 bits.

  - Disable Active Scripting if your organization requires a high level of security. **Note:** Disabling ActiveX will prevent Microsoft's automatic update sites from working properly.

- Office 2000 Productivity Applications
  - Frequently update Office applications.
  - Set macro security level to HIGH.
  - Digitally sign safe macros used within your environment.
  - Enforce installed Add-ins with the same security requirements as opening documents.
  - Protect temporary files created by Office 2000 applications.

This page intentionally left blank

11. Remote System Seat Management

Windows 2000 Active Directory includes many built-in features for the rapid deployment of software, service packs, OSs, and patches. Using the Windows 2000 built-in features is the preferred method of software update and deployment in small to medium-size environments. For organizations with large-scale environments, add-on solutions such as Microsoft's Systems Management Server (SMS) 2.0 or Intel's LanDesk 6.0 will integrate into the existing Windows 2000 Active Directory structure to provide a robust environment for extremely large-scale new software deployment and update tasks.

11.1 Software Installation and Maintenance

Windows 2000 Software Installation and Maintenance provides robust just-in-time software installation and automatic repair of applications. Administrators can use this feature to upgrade applications, retire and remove earlier applications that are no longer required, and deploy service packs and OS upgrades.

Windows 2000 Group Policy is used to define software installation options that specify which software is to be deployed, upgraded, or removed from a computer. Software installation policies can be applied to both groups of users and groups of computers. These policy definitions are based on sites, domains, and OUs. Each time a computer is turned on, the computer-based software installation Group Policy is assessed and the computer is updated, if needed. Each time a user logs on to a computer, user-related software installation Group Policy is assessed, and the desktop is updated to make available the required applications.

One of the key technologies used to perform just-in-time software installation is the Windows Installer service. The Windows Installer service fully automates the process of software installation and configuration once the software is authored or repackaged to make use of the service.

Software can either be published or assigned to users and computers by the use of Group Policy. Published software is made available to users based on their assigned OU. Users can install the published software by using the Add/Remove Programs control panel tool or by opening a document requiring one of the published applications. The required software is installed automatically, the application starts, and the file opens.

Assigning software to users and computers mandates that the software be installed. When software is assigned to a computer, the software is installed the next time the computer is rebooted. This feature can be used to deploy service packs, driver updates, and other computer-related software. When software is assigned to a user, the software appears on the user's desktop the next time the user logs in to the domain. The software is installed when the user first uses the software or a document requiring it.

When using the Windows Installer service, after applications are installed, they are protected from inadvertent deletion of application files or other required resources. Each time an application is launched, the Windows Installer service checks to ensure that all the required application files and components are available. If any are missing, the Windows Installer service retrieves and installs the missing components from a predetermined distribution point.

Remote OS Installation uses the Pre-Boot eXecution Environment (PXE) DHCP–based remote boot technology to initiate installation of an operating system from a remote source to a client's local hard disk. The remote source—a server that supports the Remote Installation Services (RIS)—provides the network equivalent of a CD-based installation of Windows 2000 Professional and preconfigured Sysprep desktop images.

11.2 Change and Configuration Management

With User and Computer Settings Management, computing environments for groupings of users and computers can be centrally defined, and they automatically get the correct environment. New users and computers can be added, settings can be defined for groups of people and computers, and changes applied for groups of people. User settings can be restored if a computer fails, and settings can be configured to roam so the user's desktop remains the same at multiple computers.

Windows 2000 Change and Configuration Management includes functionality that allows central definition of specific computing environments for groups of users and computers. This includes settings for software policies, scripts, software installation, customized user settings, and security.

Group Policy can be used to define settings for groups of users and computers. These settings include registry settings on the desktop, scripts, software installation options, and security settings.

11.3 Add-On Management Software

Software is available for Windows 2000 environments that allows for remote management and software installation within a large-scale environment. The management software greatly extends the management features offered by a Windows 2000 Active Directory Server. Two examples of this software are SMS 2.0 and LanDesk 6.0. The additional security management features provided by these software packages are described below. A huge benefit over the built-in Windows 2000 management tools is the add-on management software's ability to interoperate with all versions of the Windows OS plus the Novell directory structure.

Hardware and Software Inventory. The management software provides detailed hardware and software inventory information. The inventory provides a dynamic, efficient mechanism for obtaining hardware and software information from every application on every computer. The inventory database is then used by the management software to dynamically determine whether a computer needs a software update and whether the hardware can handle it. It also provides an up-to-date inventory for asset management.

Software Distribution and Installation. Applications can be deployed to computers, users, and user groups. Software Distribution is rules based, and distribution targets are dynamically evaluated. It is also fully integrated with the inventory to allow sophisticated targeting. If a computer logs into the network and contains an out-of-date version of software, according to the rules created by the SA, the inventory will be reviewed for hardware information to determine if the update can be safely applied, then the software will be updated. Software Distribution can be used to push or pull patches, updates, new OSs, virus definition files, etc.

Software Metering. Management servers can monitor, analyze, and if required, control the use of applications on servers and workstations. These tools provide varying levels of control, ranging from simple alerts to the ability to prevent applications from running.

Diagnostics and Troubleshooting. In addition to reporting on the current state of a workstation or server and providing remote control facilities, network tools are integrated with the management systems to analyze network and application health within the environment.

12. Conclusion

The National Institute for Standards and Technology (NIST) produced the *Systems Administration Guidance for Securing Microsoft Windows 2000 Professional System* to assist personnel responsible for the administration and security of Windows 2000 Professional (Win2K Pro) systems. This guide is intended for *managed environments* and should not be applied throughout an enterprise unless trained and competent systems administrators (SA) are available on the staff. Experienced SAs in these managed environments may use this guide to secure local Win2K Pro workstations, Win2K Pro mobile computers, and Win2K Pro computers used by telecommuters. NIST recommends that users who are directly applying this guide to secure their computers have significant competence in the administration of Windows systems.

The guide provides detailed information about the security features of Win2K Pro, security configuration guidelines for popular applications, and security configuration guidelines for the Win2K Pro operating system. The guide documents the methods that SAs can use to implement each security setting recommended. The principal goal of the document is to recommend and explain tested, secure settings for Win2K Pro workstations with the objective of simplifying the administrative burden of improving the security of Win2K Pro systems. It is strongly recommended that these settings be tested on non-production systems before being deployed.

The recommendations presented herein are not intended to imply, mention, refer to, or voice a commercial recommendation for any of the involved technology whatsoever.

This page intentionally left blank

Appendix A—Registry Discussion

Appendix A presents a brief overview of the Windows 2000 registry. This discussion assumes that the reader has some degree of familiarity with interacting with the registry through tools such as the Windows Registry Editor **regedit32.exe**, and registry scripts (those scripts with a **.reg** extension). In reality, with the applications programming interfaces (API) that Microsoft and third-party organizations have developed, numerous ways exist to access the registry statically and in real-time.

The Windows 2000 registry is a binary database that holds settings and configuration information that the Windows 2000 operating system (OS) requires to function. It is created in memory from a set of data files on the hard disk each time the machine starts. The registry is continually maintained in memory until the system is powered down. Because the registry could conceivably grow very large and must be able to be accessed quickly for performance reasons, the data within the registry is stored in binary format as opposed to text format like earlier versions of Windows.

The registry is organized into the following four levels, in a descending hierarchy:

- **Hive Keys.** These keys, which are system-defined and prefixed with the letters **HKEY_**, act as organizational assistants. Microsoft divides any subkeys based on purpose. The five hive keys are listed in Table A-1.

Table A-1. Hive Keys

HKEY_LOCAL_MACHINE (HKLM). This hive contains operating system and hardware-oriented information. HKLM holds most of the information of the registry because two of the other four hive keys are aliased to its subkeys.
HKEY_CURRENT_USER (HKCU). This hive contains the user profile for the specific user who is currently logged into the system.
HKEY_CLASSES_ROOT (HKCR). This hive contains subkeys listing all COM servers currently registered on the computer and all file extensions currently associated with applications.
HKEY_USERS (HKU). This hive contains subkeys that contain all the user profiles for the current computer.
HKEY_CURRENT_CONFIG (HKCC). This hive contains subkeys listing all the hardware profile information for the current session of the computer.

- **Keys.** Keys can be either user- or system-defined and have no strict naming convention. They function as an additional level of organization for subsequent values.
- **Sub-keys.** Subkeys are yet another level of organization for subsequent values. Like keys, they have no strict naming convention.
- **Values** – These are the lowest elements in the hierarchy and contain actual data that is used by the operating system and applications.

The Windows 2000 registry uses a schema to specify its structure and organization, and this is accomplished in part using a restricted set of data types that registry values can contain. Table A-2 lists the recognized data types for the Windows 2000 registry.

Table A-2. Recognized Data Types for Windows 2000 Registry

Name	Underlying Representation	Function
REG_NONE	Unknown	Encrypted data
REG_SZ	String	Text characters
REG_EXPAND_SZ	String	Text variables
REG_BINARY	Binary	Binary data
REG_DWORD	Number	Numerical data
REG_DWORD_BIG_ENDIAN	String	Non-Intel numbers
REG_LINK	String	Path to a file
REG_MULTI_SZ	Multistring	String arrays
REG_RESOURCE_LIST	String	Hardware resource list
REG_FULL_RESOURCE_DESCRIPTOR	String	Hardware resource ID
REG_RESOURCE_REQUIREMENTS_LIST	String	Hardware resource ID

Note that the Windows 2000 Professional registry must be backed up on a regular basis. This is another concept in the administration of Windows 2000 machines whose importance cannot be emphasized enough. Backups should reflect the criticality level that a machine serves within an organizations infrastructure and business practice. These backups should be stored on alternate storage media such as compact disc (CD), tape, or even Iomega Zip disks if necessary.

Microsoft includes a new method of accessing the Windows 2000 registry in the Windows 2000 Resource Kit, the command-line utility **reg.exe**. This utility is native to Windows 2000 and includes the following capabilities:

- Adding new registry keys
- Updating information in existing registry keys
- Removing registry keys
- Saving registry keys to hive files
- Finding specific registry keys or values.

A discussion of security of the Windows 2000 Professional registry should include a review of its default access control list (ACL) settings. Adding, deleting, and changing the values within the registry are not the only processes to enhance system security. More keys and values within the registry store data that is of a sensitive nature to system users than can be mentioned in one discussion. It is important to understand the default restrictions on the registry hives because a user will be able to determine a plan of action if it is necessary to change ACL settings later. Table A-3 lists the default registry ACLs for Windows 2000 Professional.

The following conventions help explain the information provided in Table A-3.

- SW stands for Software

- MS stands for Microsoft
- W stands for Windows
- W NT stands for Windows NT
- CV stands for Current Version.

Table A-3. Default Registry ACLs

Registry Key/Hive	Default User Permissions
HKEY_LOCAL_MACHINE	
HKLM\Software	Read
HKLM\SW\Classes\helpfile	Read
HKLM\SW\Classes\.hlp	Read
HKLM\SW\MS\Command Processor	Read
HKLM\SW\MS\Cryptography	Read
HKLM\SW\MS\Driver Signing	Read
HKLM\SW\MS\EnterpriseCertificates	Read
HKLM\SW\MS\Non-Driver Signing	Read
HKLM\SW\MS\NetDDE	None
HKLM\SW\MS\Ole	Read
HKLM\SW\MS\Rpc	Read
HKLM\SW\MS\Secure	Read
HKLM\SW\MS\SystemCertificates	Read
HKLM\SW\MS\Windows\CV\RunOnce	Read
HKLM\SW\MS\W NT\CV\DiskQuota	Read
HKLM\SW\MS\W NT\CV\Drivers32	Read
HKLM\SW\MS\W NT\CV\Font Drivers	Read
HKLM\SW\MS\W NT\CV\FontMapper	Read
HKLM\SW\MS\W NT\CV\Image File Execution Options	Read
HKLM\SW\MS\W NT\CV\IniFileMapping	Read
HKLM\SW\MS\W NT\CV\Perflib	Read (via Interactive)
HKLM\SW\MS\W NT\CV\SecEdit	Read
HKLM\SW\MS\W NT\CV\Time Zones	Read
HKLM\SW\MS\W NT\CV\Windows	Read
HKLM\SW\MS\W NT\CV\AsrCommands	Read
HKLM\SW\MS\W NT\CV\Winlogon	Read
HKLM\SW\MS\W NT\CV\Classes	Read
HKLM\SW\MS\W NT\CV\Console	Read
HKLM\SW\MS\W NT\CV\ProfileList	Read
HKLM\SW\MS\W NT\CV\Svchost	Read
HKLM\SW\Policies	Read
HKLM\System	Read

Registry Key/Hive	Default User Permissions
HKLM\SYSTEM\CCS\Control\SecurePipeServers\winreg	None
HKLM\SYSTEM\CCS\Control\Session Manager\Executive	Read
HKLM\SYSTEM\CCS\Control\TimeZoneInformation	Read
HKLM\SYSTEM\CCS\Control\WMI\Security	None
HKLM\Hardware	Read (via Everyone)
HKLM\SAM	Read (via Everyone)
HKLM\Security	None
HKEY_USERS	
USERS\.DEFAULT	Read
USERS\.DEFAULT\SW\MS\NetDDE	None
HKEY_CURRENT_CONFIG	
HKEY_CURRENT_USER	Full Control
HKEY_CLASSES_ROOT	

Note: Do not change any Access Control Entry on a registry hive without being fully aware of the consequences.

Description of Modified Keys

This section discusses the keys modified by the security checklist for Windows 2000 Professional included in Appendix B. Table A-4 describes the Windows 2000 Professional registry keys in detail.

Table A-4. Keys Modified by NIST template

Description and Data Type of Registry Keys		
Registry Value:	HKEY_LOCAL_MACHINE\SOFTWARE\Windows NT\CurrentVersion\Winlogon\SFCShowProgress	
Hides the Windows File Protection progress display window from the user.		REG_DWORD

Registry Value:	HKEY_LOCAL_MACHINE\Software\microsoft\driver signing\policy	
Configures Windows 2000 to display a warning when it encounters a driver that has not been signed or has been signed incorrectly.		REG_BINARY

Registry Value:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DrWatson\CreateCrashDump	
Disables the creation of a memory dump file by Dr. Watson. Memory dumps can contain sensitive and often critical information such as passwords. Any memory dump that is found and is not needed for purposes should be promptly deleted.		REG_DWORD

Registry Value:	HKEY_LOCAL_MACHINE\software\microsoft\non-driver signing\policy	
Configures Windows 2000 to display an alert when it encounters a hardware item without a digital signature.		REG_BINARY

Registry Value:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\WinlogonDontDisplayLastUserName	
Blanks the username box on the logon screen. Preventing users who are logging on from knowing the last user to access the system. Upon creating/modifying this value, exit the registry. The machine may need to be restarted for the change to take effect.		REG_SZ

Registry Value:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug\Auto	
Disables the Dr. Watson program debugger on Windows 2000 Professional. To reenable the debugger, type the following at the command line: C:\>drwtsn –I		REG_DWORD

Registry Value:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SFCDisable	
Concerns Windows File Protection (WFP) and System File Checker (SFC). The setting of 4 means that WFP/SFC is enabled but with popups disabled.		REG_DWORD

Registry Value:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SFCScan	
Configures the SFC to scan the protected files at every boot. This process is resource intensive, but there is a direct tradeoff with security. Implement a key like this only after serious consideration.		REG_DWORD

Registry Value:	HKEY_LOCAL_MACHINE\Software\Microsoft\windows nt\currentversion\winlogon\allocatecdroms

Description and Data Type of Registry Keys	
Determines whether data in the CD-ROM drive is accessible to other users. This value entry satisfies, in part, the command and control security requirement that the user must be able to secure removable media. A value of 0 indicates that CDs in the CD-ROM drive can be accessed by all administrators in the domain. A value of 1 means that only the user logged on locally can access data on the CDs in the CD-ROM drive.	REG_SZ

Registry Value:	HKEY_LOCAL_MACHINE\Software\Microsoft\windows nt\currentversion\winlogon\allocatedasd
Determines which types of users can format/eject a removable hard disk.	REG_SZ

Registry Value:	HKEY_LOCAL_MACHINE\Software\Microsoft\windows nt\currentversion\winlogon\allocatefloppies
Determines whether data in the floppy disk drive is accessible to other users. This value entry satisfies, in part, the C2 security requirement that you must be able to secure removable media. A value 0 means that floppy disks in the floppy disk drive can be accessed by all administrators in the domain. A value of 1 means that only the user logged on locally can access data on the floppy disks in the floppy disk drive.	REG_SZ

Registry Value:	HKEY_LOCAL_MACHINE\Software\Microsoft\windows nt\currentversion\winlogon\cachedlogonscount
Determines the number of previous logons that the OS will cache if a domain controller cannot be contacted. When set to 0, users will be unable to log on to their domain account unless a domain controller is available. If domain logon is required when the domain controller is down, set this value to the number of users normally using the computer.	REG_DWORD

Registry Value:	HKEY_LOCAL_MACHINE\Software\Microsoft\windows nt\currentversion\winlogon\passwordexpirywarning
Displays a warning to users when their passwords are about to expire. The amount of time before this warning is given can be set in the value.	REG_BINARY

Registry Value:	HKEY_LOCAL_MACHINE\Software\Microsoft\windows nt\currentversion\winlogon\scremoveoption
Controls whether users can remove smart cards from readers. Removing smart cards has been shown to cause applications that use smart cards to behave insecurely; therefore, users should be prevented from doing so.	REG_DWORD

Registry Value:	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AutoAdminLogon
Provides an ability to bypass the logon prompt. The setting stores the associated password in clear-text within the registry and is viewable by all users with the appropriate permissions. It is recommended that this setting be disabled because of the security implications of its misuse.	REG_SZ

Registry Value:	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\NetworkHideSharePwds
Controls whether the password typed when accessing a file share is shown in clear text or as asterisks. This option can be useful in a peer-to-peer network environment of Windows 2000 machines.	REG_DWORD

Registry Value:	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\NetworkNoDialIn

Description and Data Type of Registry Keys	
It is possible for users to set up a modem on a Windows machine; by using Dial-up Networking, callers can connect to the internal network. Especially in a corporate environment, this action can cause a major security risk. Exit your registry; you may need to restart or log out of Windows before the change will take effect.	REG_DWORD

Registry Value:	HKEY_LOCAL_MACHINE\Software\Microsoft\windows\currentversion\policies\System\ disablecad
Determines whether users must press the Ctrl+Alt+Del security attention sequence to log on to Windows 2000. Enabling this setting is not recommended because the secure attention sequence can bypass Trojan logon prompts. Never log into a computer that displays the logon prompt automatically; always press Ctrl+Alt+Del to display it.	REG_DWORD

Registry Value:	HKEY_LOCAL_MACHINE\Software\Microsoft\windows\currentversion\policies\System\ dontdisplaylastusername
Prevents the logon screen from displaying the last known user who logged into the system. Although this information does not directly influence system security, it is an issue of privacy to prevent this information from being available to anyone with physical access to the machine.	REG_DWORD

Registry Value:	HKEY_LOCAL_MACHINE\Software\Microsoft\windows\currentversion\policies\System\ shutdownwithoutlogon
Prevents the user from being allowed to activate the shutdown feature from the logon screen without having to supply a password. This maintains the computer security principle of availability.	REG_DWORD

Registry Value:	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explor er\NoDriveTypeAutoRun
Disables the autorun feature of the CD-ROM drive. This feature is useful when dealing with discs whose integrity cannot be trusted. Certain applications also claim to have unpredictable behavior when installing on a CD with autorun enabled.	REG_DWORD

Registry Value:	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControlAutoRebo ot
Some sites believe that security is enhanced and important information preserved intact (security event logs), if systems are not allowed to restart automatically after a failure or lockup. This is not useful for machines that serve in “always-on” mode where the machine is depended on to be running around the clock for some critical service it provides.	REG_DWORD

Registry Value:	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\RestrictAnonymous
The Red Button access attack uses Anonymous User Connections, also called Null User Connections, to discover which account is the administrative account and what the network shares are. The user can disable this discovery by preventing anonymous connections to domains using the following Windows NT registry hack. Caution: this measure can have severe consequences on Structured Query Language (SQL) server access, as well as on creating and maintaining domain trusts.	REG_DWORD

Registry Value:	HKEY_LOCAL_MACHINE\System\CurrentControlSet\control\session manager\memory management\clearpagefileatshutdown

Description and Data Type of Registry Keys	
Specifies that the memory page file pagefile.sys will be cleared each time the machine is powered down preventing data reminisce. Because the pagefile is inaccessible during runtime, it is unnecessary to clear it while the computer is on. **Note:** This setting should be enabled or disabled according to your organizational security policy.	REG_DWORD

Registry Value:	HKEY_LOCAL_MACHINE\System\CurrentControlSet\control\session manager\protectionmode
Adds strong protection over shared objects. It will prevent users from unauthorized access to the known dynamic link library (DLL) lookup table.	REG_DWORD

Registry Value:	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\ParametersAutoShareWks
When networking has been installed on a Windows 2000 machine, it will automatically create hidden shares to the local disk drives. The shares are normally accessed via \\server\c$ and \\server\d$ depending on the drive letter. It is possible to disable the sharing at run-time, but this registry value will stop the automatic sharing altogether.	REG_DWORD

Registry Value:	HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\lanmanserver\parameters\enableforcedlogoff
Enables the OS to perform a forced logoff of a user who is logged into Windows 2000 Professional.	REG_DWORD

Registry Value:	HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\lanmanserver\parameters\enablesecuritysignature
Enables the OS to digitally sign all network SMB traffic to servers.	REG_DWORD

Registry Value:	HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\lanmanworkstation\parameters\enablesecuritysignature
Enables the OS to digitally sign all network SMB traffic to clients.	REG_DWORD

Registry Value:	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MrxSmb\ParametersRefuseReset
It is possible for a malicious user to shut down a computer browser, or all computer browsers, on the same subnet. If all of the computers on the same subnet are shut down, they can then declare their own computer the new master browser. Microsoft has published a patch for this vulnerability which can be found at: http://www.microsoft.com/windows2000/downloads/critical/q262694/default.asp	REG_DWORD

Registry Value:	HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\netlogon\parameters\requiresignorseal
Specifies the requirement of securing the communications, by encrypting or digitally signing, between a client and a domain controller.	REG_DWORD

Registry Value:	HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\netlogon\parameters\requirestrongkey
Requires a strong key for communications between a client and a domain controller.	REG_DWORD

Registry Value:	HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\netlogon\parameters\sealsecurechannel
Requires encrypting the communications between a client and domain controller.	REG_DWORD

Description and Data Type of Registry Keys	
Registry Value:	HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\netlogon\parameters\signsecurechannel
Requires digitally signing the communications between a client and domain controller.	REG_DWORD

Registry Value:	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableDeadGWDetect
When this parameter is set to 1, TCP is allowed to perform dead-gateway detection. With this feature enabled, TCP may ask IP to change to a backup gateway if a number of connections are experiencing difficulty. Backup gateways may be defined in the Advanced section of the TCP/IP configuration dialog in the Network Control Panel.	REG_DWORD

Registry Value:	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirect
Controls whether Windows 2000 will alter its route table in response to Internet Control Message Protocol (ICMP) redirect messages that are sent to it by network devices such as a routers.	REG_DWORD

Registry Value:	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnablePMTUDiscovery
When this parameter is set to 1, TCP attempts to discover the Maximum Transmission Unit (MTU or largest packet size) over the path to a remote host. By discovering the Path MTU and limiting TCP segments to this size, TCP can eliminate fragmentation at routers along the path that connect networks with different MTUs. Fragmentation adversely affects TCP throughput and network congestion. Setting this parameter to 0 causes an MTU of 576 bytes to be used for all connections that are not to hosts on the local subnet.	REG_DWORD

Registry Value:	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTime
The KeepAliveTime parameter controls how often TCP attempts to verify that an idle connection is still intact by sending a keep-alive packet. If the remote system is still reachable and functioning, it acknowledges the keep-alive transmission. Keep-alive packets are not sent by default. This feature may be enabled on a connection by an application.	REG_DWORD

Registry Value:	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\NoNameReleaseOnDemand
The NoNameReleaseOnDemand parameter determines whether the computer releases its NetBIOS name when it receives a name-release request from the network. It was added to allow the SA to protect the machine against malicious name-release attacks.	REG_DWORD

Registry Value:	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\PerformRouterDiscovery
This parameter controls whether Windows 2000 attempts to perform router discovery per RFC 1256 on a per-interface basis.	REG_DWORD

Registry Value:	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect
Provides reduced retransmission retries and delayed route cache entry (RCE) creation if the TcpMaxHalfOpen and TcpMaxHalfOpenRetried settings are	REG_DWORD

Description and Data Type of Registry Keys	
satisfied and adds delayed indication to Winsock to setting of 1.	

Registry Value:	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Tcp MaxHalfOpen
Controls the number of connections in the SYN-RCVD state allowed before SYN-ATTACK protection begins to operate. If SynAttackProtect is set to 1, ensure that this value is lower than the afd.sys listen backlog on the port you want to protect.	REG_DWORD

Registry Value:	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Tcp MaxHalfOpenRetried
The TcpMaxHalfOpenRetried parameter controls the number of connections in the SYN-RCVD state for which at least one retransmission of the SYN has been sent, before SYN-ATTACK attack protection begins to operate.	REG_DWORD

Appendix B—NIST Windows 2000 Security Templates

Appendix B discusses security templates for Windows 2000 as shown in Table B-1. This document provides sample security templates for use with Windows 2000 Professional, for both domain members and stand-alone machines. Because of the extremely large diversity of computing environments, exercise caution when applying these templates to an installation of Windows 2000 Professional. **The current version of this appendix and the security templates can be downloaded from the following page:**
http://csrc.nist.gov/itsec/guidance_W2Kpro.html

Table B-1. Sample Windows 2000 Security Templates

Template	Description
NISTWin2kProGold.inf	This template is designed for stand-alone installations of Windows 2000 Professional. The template contains all of the settings included in the consensus baseline.
NISTWin2kProGoldPlus.inf	This template includes all the settings found in the NISTWin2kProGold.inf template and adds some additional restrictions on various executables. This template provides added protection for sites that require it.

Users who examine these templates will find some settings disabled by default. Although enabling these settings is recommended for security reasons, it is important to note that when enabled, they cause loss of functionality within Windows 2000. Consult the templates listed in Table B-1 for a further explanation.

Although these templates have been tested, extreme care should be taken when applying these templates to Windows 2000 Professional. These templates will not work on Windows 2000 server or Windows XP.

Template Security Settings

Listed below are the settings and descriptions included in the NIST .inf files. The actual entries included in the .inf files are shown in Boldface. Each setting is numbered and corresponds to an entry in the .inf file.

B.1 General Description

This section of the template provides information about the name and creation date of the template. It includes an introduction, general disclaimer, and links to various organizations that have contributed to the development of the template.

B.2 Revision History

This section lists the changes that were made to the template.

B.3 Security Settings

This section represents all the settings that will be applied to the system.

B.3.1 Account Policies

Tables B-2, B-3, and B-4 define parameters for account security and password policy. They correspond to the Account policies section of the Local Security policy MMC snap-in.

Table B-2. Parameters for the Password Policy

	Password Policy	Recommended Settings	Comments
3.1.1.1	**Enforce password history**	24 passwords remembered	
3.1.1.2	**Maximum password age**	90 days	Reduce the maximum number of days before users must change passwords for compliance with local security policy. Increasing the number of days beyond the recommended setting is highly discouraged.
3.1.1.3	**Minimum password age**	1 day	
3.1.1.4	**Minimum password length**	8 characters	Increase the minimum password length for compliance with local security policy and greater security. Decreasing the password length below the recommended setting is highly discouraged.
3.1.1.5	**Passwords must meet complexity requirements**	Enabled	Use the default Microsoft filer or enpasflt.dll, the NSA password filter, or a third-party password filter.
3.1.1.6	**Store password using reversible encryption for all users in the domain**	Disabled	

Table B-3. Parameters for the Account Lockout Policy

	Account Lockout Policy	Recommended Settings	Comments
3.1.2.1	**Account lockout duration**	15 minutes	Modify the account lockout settings for compliance with local security policy. Disabling account lockout entirely is highly discouraged.
3.1.2.2	**Account lockout threshold**	3 invalid logon attempts	Increase this parameter to a higher value before a vulnerability scan is performed.
3.1.2.3	**Reset account lockout counter after**	15 minutes	

Table B-4. Requirement to Change an Existing Password

3.1.3.1	**Require logon to change the password**	Enabled	This parameter required that the users be logged on a system before they can change their password. If a password has expired and the users are currently not logged on a system, an SA must log on to change the user password.

B.3.2 Local Policies

The Local Policies area of the template defines the policies for the system auditing policy, user rights assignment, and security options as shown in tables B-5, B-6, and B-7. These tables define the NIST template settings.

Table B-5. Parameters for the Audit Policy

	Audit Policy	Recommended Settings	Comments
3.2.1.1	**Audit account logon events**	Success, Failure	
3.2.1.2	**Audit account management**	Success, Failure	
3.2.1.3	**Audit directory service access**		
3.2.1.4	**Audit logon events**	Success, Failure	
3.2.1.5	**Audit object access**	Failure	Determines whether to audit the event of a user accessing an object (e.g., a file, folder, registry key, or printer) that has its own system access control list (SACL) specified. SACL can be set on a file system object using the **Security** tab in that object's **Properties** dialog box.

	Audit Policy	Recommended Settings	Comments
3.2.1.6	**Audit policy change**	Failure	Determines whether to audit every incidence of a failed attempt to change user rights assignment policies, audit policies, or trust policies. Adding success to this setting will increase not only log entries, but also the system activity tracking capability.
3.2.1.7	**Audit privilege use**	Failure	Note that it is likely to generate a very large number of events.
3.2.1.8	**Audit process tracking**		
3.2.1.9	**Audit system events**	Success, Failure	

Table B-6. Parameters for the User Rights Assignment

	User Rights Assignment	Recommended Settings	Comments
3.2.2.1	**Access this computer from the network**	Users, Administrators	Remove users and administrators from this setting if local workstations do not share files, folders, or printers and if remote administration is not desired.
3.2.2.2	**Act as part of the operating system**	None	
3.2.2.3	**Add workstations to domain**	None	
3.2.2.4	**Back up files and directories**	Administrators	Add other user groups as required by the local policy.
3.2.2.5	**Bypass traverse checking**	Users	
3.2.2.6	**Change the system time**	Administrators	
3.2.2.7	**Create a pagefile**	Administrators	
3.2.2.8	**Create a token object**	None	
3.2.2.9	**Create permanent shared objects**	None	
3.2.2.10	**Debug programs**	None	
3.2.2.11	**Deny access to this computer from the network**	Guests	
3.2.2.12	**Deny logon as a batch job**	None	
3.2.2.13	**Deny logon as a service**	None	
3.2.2.14	**Deny logon locally**	None	

	User Rights Assignment	Recommended Settings	Comments
3.2.2.15	**Enable computer and user accounts to be trusted for delegation**	None	
3.2.2.16	**Force shutdown from a remote system**	Administrators	
3.2.2.17	**Generate security audits**	None	
3.2.2.18	**Increase quotas**	Administrators	
3.2.2.19	**Increase scheduling priority**	Administrators	
3.2.2.20	**Load and unload device drivers**	Administrators	
3.2.2.21	**Lock pages in memory**	None	
3.2.2.22	**Log on as a batch job**	None	
3.2.2.23	**Log on as a service**	None	
3.2.2.24	**Log on locally**	Users, Administrators	
3.2.2.25	**Manage auditing and security log**	Administrators	Add other user groups as required by the local policy.
3.2.2.26	**Modify firmware environment values**	Administrators	
3.2.2.27	**Profile single process**	Administrators	
3.2.2.28	**Profile system performance**	Administrators	
3.2.2.29	**Remove computer from docking station**	Users, Administrators	
3.2.2.30	**Replace a process level token**	None	
3.2.2.31	**Restore files and directories**	Administrators	Add other user groups as required by the local policy.
3.2.2.32	**Shut down the system**	Users, Administrators	
3.2.2.33	**Synchronize directory service data**	None	
3.2.2.34	**Take ownership of files or other objects**	Administrators	

Table B-7. Parameters for the Security Options

	Security Options	Recommended Settings	Comments
3.2.3.1	**Additional restrictions for anonymous connections**	No access without explicit anonymous permissions	This can break some legacy applications. Try backing down to "Do Not allow Enumeration…" and rebooting to see if that will resolve individual problems. Only back down to the default setting if absolutely necessary.
3.2.3.2	**Allow server operators to schedule tasks (domain controllers only)**	Not defined	
3.2.3.3	**Allow system to be shut down without having to log on**	Disabled	If your organization local policy and security risk level does not require logging of shutdown events, this setting can be enabled.
3.2.3.4	**Allowed to eject removable NTFS media**	Administrators	
3.2.3.5	**Amount of idle time required before disconnecting session**	30 minutes	Reduction of this setting increases the number of times that transmission of credentials occurs across the network and increases network traffic. In some cases, users are required to manually log in after disconnection from a session. Adjust this setting to comply with local security policy; increasing this setting is discouraged.
3.2.3.6	**Audit the access of global system objects**	Disabled	If this policy is enabled, it causes system objects, such as mutexes, events, semaphores, and DOS devices, to be created with a default SACL. If the Audit object access audit policy is also enabled, access to these system objects is audited. Enabling this setting greatly increases log entries. Warning: Enabling this option will generate many log events and cause the log file to fill rapidly.
3.2.3.7	**Audit use of Backup and Restore privilege**	Disabled	Warning: Enabling this option will generate many log events and cause the log file to fill rapidly.
3.2.3.8	**Automatically log off users when logon time expires**	Enabled	
3.2.3.9	**Automatically log off users when logon time expires (local)**	Enabled	
3.2.3.10	**Clear virtual memory pagefile when system shuts down**	Enabled	The virtual memory pagefile stores information accessed during a users session. The pagefile can contain potentially sensitive data. Enabling the setting causes a workstation shutdown to take minimally longer to complete.
3.2.3.11	**Digitally sign client communication (always)**	Not defined	

	Security Options	Recommended Settings	Comments
3.2.3.12	**Digitally sign client communication (when possible)**	Enabled	
3.2.3.13	**Digitally sign server communication (always)**	Not defined	
3.2.3.14	**Digitally sign server communication (when possible)**	Enabled	
3.2.3.15	**Disable CTRL+ALT+DEL requirement for logon**	Disabled	
3.2.3.16	**Do not display last user name in logon screen**	Enabled	SAs can disable this option if they wish to allow users to determine if anyone else has logged on to the user's workstation when he or she was not present.
3.2.3.17	**LAN Manager (LM) Authentication Level**	Send NTLMv2 response only	Using this setting will prevent legacy client systems and legacy applications from connecting to the Windows 2000 system. Communication with Windows 9x/Me systems will require the use of the DSCLIENT.EXE utility found on the Windows 2000 installation CD-Rom. If LM Authentication is required, configure this parameter to "Send LM & NTLM - Use NTLMv2 session security if negociated" value.

	Security Options	Recommended Settings	Comments
3.2.3.18	**Message text for users attempting to log on**	This system is for the use by 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 who are 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	Replace the sample DOJ logon banner with a local approved banner.

[1] http://www.cert.org/advisories/CA-1992-19.html

	Security Options	Recommended Settings	Comments
		evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.[1]	
3.2.3.19	**Message title for users attempting to log on**	--- WARNING ---	Insert title of the logon banner window here.
3.2.3.20	**Number of previous logons to cache (in case domain controller is not available)**	1 logon	One logon is cached for each user logging on to the system. This situation allows users to log into domain accounts, even if the domain controller is offline. The caching of credentials on the local workstation presents a slight risk, but adds increased availability of services. Change to a higher value for a portable system that may be disconnected from the domain for an extended period of time.
3.2.3.21	**Prevent system maintenance of computer account password**	Disabled	
3.2.3.22	**Prevent users from installing printer drivers**	Enabled	Printer drivers can be potentially Trojaned by an attacker; enabling this setting allows SAs control over the verification and installation of printer drivers.
3.2.3.23	**Prompt user to change password before expiration**	14 days	
3.2.3.24	**Recovery Console: Allow automatic administrative logon**	Disabled	
3.2.3.25	**Recovery Console: Allow floppy copy and access to all drives and all folders**	Disabled	
3.2.3.26	**Rename administrator account**	Not defined	Rename the Administrator account. It can protect against a scripted attack.
3.2.3.27	**Rename guest account**	Not defined	Rename the Guest account.
3.2.3.28	**Restrict CD-ROM access to locally logged-on user only**	Enabled	If the users try to install software from a CD-ROM drive and the installation packages use the Microsoft Installer (.MSI) packages, the installation will fail because the software is actually installed by the Windows Installer service. It

	Security Options	Recommended Settings	Comments
			is recommended that the users copy the installation packages to a network or local drive for the installation procedure to succeed.
3.2.3.29	**Restrict floppy access to locally logged-on user only**	Enabled	
3.2.3.30	**Secure channel: Digitally encrypt or sign secure channel data (always)**	Not defined	To enable this setting on a member workstation, all domain controllers in the domain to which the member belongs must be able to encrypt secure channel data with a strong (128-bit) key. Therefore, all these domain controllers must be running Windows 2000.
3.2.3.31	**Secure channel: Digitally encrypt secure channel data (when possible)**	Enabled	
3.2.3.32	**Secure channel: Digitally sign secure channel data (when possible)**	Enabled	
3.2.3.33	**Secure channel: Require strong (Windows 2000 or later) session key**	Not defined	To enable this setting on a member workstation, all domain controllers in the domain to which the member belongs must be able to encrypt secure channel data with a strong (128-bit) key. Therefore, all these domain controllers must be running Windows 2000.
3.2.3.34	**Secure system partition (for reduced instruction set computer (RISC) platforms only)**	Not defined	
3.2.3.35	**Send unencrypted password to connect to third-party SMB servers**	Disabled	
3.2.3.36	**Shut down system immediately if unable to log security audits**	Not defined	Enable this setting in a high security risk environment.
3.2.3.37	**Smart card removal behavior**	Lock workstation	
3.2.3.38	**Strengthen default permissions of global system objects (e.g., symbolic links)**	Enabled	
3.2.3.39	**Unsigned driver installation behavior**	Warn but allow installation	The system prompts administrative group members to click on the confirmation dialog box to proceed. Members of the users' group do not have the right to install the drivers.
3.2.3.40	**Unsigned non-driver installation behavior**	Warn but allow installation	The system prompts the administrative group members to click on the confirmation dialog box to proceed. Members of the users' group do not have the right to install the nondrivers.

B.3.3 Event Log Policy Settings

For the log settings shown in Table B-8, the default maximum size is 4 gigabytes (GB) on all three logs. Although logs may never actually reach their full size, this setting should reflect the physical hard drive space that is available. Change this setting only if you are completely aware of the status of the physical log files in tandem with the audit policy of your enterprise.

Table B-8. Parameters for the Event Log Policy

	Event Log Policy	Recommended Settings	Comments
3.3.1	**Maximum application log size**	80 MB	Increase or decrease the log size to comply with local logging policy and installed hardware limitations. Recommend using the NSA log analysis program that is available to the federal and Department of Defense (DoD) community.
3.3.2	**Maximum security log size**	80 MB	Increase or decrease the log size to comply with local logging policy and installed hardware limitations. Be aware that if the log file is filled, a users' group member will be unable to log on and only an administrator will be able to reset the system.
3.3.3	**Maximum system log size**	80 MB	Increase or decrease the log size to comply with local logging policy and installed hardware limitations.
3.3.4	**Restrict guest access to application log**	Enabled	
3.3.5	**Restrict guest access to security log**	Enabled	
3.3.6	**Restrict guest access to system log**	Enabled	
3.3.7	**Retain application log**	Not defined	Change the log retention policy to comply with local log retention policy and procedures.
3.3.8	**Retain security log**	Not defined	Change the log retention policy to comply with local log retention policy and procedures. Be aware that if the log file is filled, a users' group member will be unable to log on and only an administrator will be able to reset the system.
3.3.9	**Retain system log**	Not defined	Change the log retention policy to comply with local log retention policy and procedures.
3.3.10	**Retention method for application log**	Overwrite events as needed	Change the log retention policy to comply with local log retention policy and procedures.

	Event Log Policy	Recommended Settings	Comments
3.3.11	**Retention method for security log**	Overwrite events as needed	Change the log retention policy to comply with local log retention policy and procedures.
3.3.12	**Retention method for system log**	Overwrite events as needed	Change the log retention policy to comply with local log retention policy and procedures.
3.3.13	**Shut down the computer when the security audit log is full**	Not Defined	Enable this setting in a high security risk environment.

B.3.4 Restricted Groups

The Restricted Groups Policy area of the template is for administration of local groups. The recommended settings for the NIST template are shown in Table B-9. NIST recommends removing all members from the Power Users group. If local policy requires the usage of the Power Users group be certain to add the users requiring membership to the following setting.

Table B-9. Restricted Groups Settings

	Restricted Groups	Comments
3.4.1	Power Users	The Restricted Groups remove all users from the Power Users group unless they are manually entered into the inf file.

B.3.5 System Services

The recommended method of starting various System Services is defined in Table B-10.

Table B-10. System Services Settings

	Service Name	Recommended Settings	Comments
3.5.1	**Alerter**	Disabled	
3.5.2	**Application Management**	Not defined	
3.5.3	**ClipBook**	Disabled	
3.5.4	**COM+ Event System**	Not defined	
3.5.5	**Computer Browser**	Disabled	Disabling the service prevents the user from browsing the network neighborhood. In addition, block all ingress and egress NetBIOS traffic and restrict anonymous access at the border router and gateway firewall.

	Service Name	Recommended Settings	Comments
3.5.6	**DHCP Client**	Not defined	
3.5.7	**Distributed Link Tracking Client**	Not defined	
3.5.8	**Distributed Transaction Coordinator**	Not defined	
3.5.9	**DNS Client**	Not defined	
3.5.10	**Event Log**	Not defined	
3.5.11	**Fax Service**	Disabled	
3.5.12	**FTP Publishing Service**	Disabled	
3.5.13	**IIS Admin Service**	Disabled	
3.5.14	**Indexing Service**	Not defined	
3.5.15	**Infrared Monitor**	Not defined	
3.5.16	**Internet Connection Sharing**	Disabled	
3.5.17	**IPsec Policy Agent**	Not defined	
3.5.18	**Logical Disk Manager**	Not defined	
3.5.19	**Logical Disk Manager Administrative Service**	Not defined	
3.5.20	**Messenger**	Not defined	Disabling the service prevents the user from receiving administrative alerts.
3.5.21	**MSSQLServer**	Not defined	Disable and uninstall the MS SQL server if it is not required.
3.5.22	**Net Logon**	Not defined	
3.5.23	**NetMeeting Remote Desktop Sharing**	Disabled	
3.5.24	**Network Connections**	Not defined	
3.5.25	**Network DDE**	Not defined	
3.5.26	**Network DDE DSDM**	Not defined	
3.5.27	**NT LM Security Support Provider**	Not defined	
3.5.28	**Performance Logs and Alerts**	Not defined	
3.5.29	**Plug and Play**	Not defined	
3.5.30	**Print Spooler**	Not defined	
3.5.31	**Protected Storage**	Not defined	
3.5.32	**QoS RSVP**	Not defined	
3.5.33	**Remote Access Auto Connection Manager**	Not defined	
3.5.34	**Remote Access Connection Manager**	Not defined	
3.5.35	**Remote Procedure Call (RPC)**	Not defined	
3.5.36	**Remote Procedure Call (RPC) Locator**	Not defined	
3.5.37	**Remote Registry Service**	Disabled	Disabling this service may break some remote administration tools, so test before full-scale deployment. The MBSA tool will not work if the service is disabled.
3.5.38	**Removable Storage**	Not defined	

	Service Name	Recommended Settings	Comments
3.5.39	**Routing and Remote Access**	Disabled	
3.5.40	**RunAs Service**	Not defined	
3.5.41	**Security Accounts Manager**	Not defined	
3.5.42	**Server**	Not defined	
3.5.43	**Simple Mail Transport Protocol (SMTP)**	Disabled	
3.5.44	**Smart Card**	Not defined	
3.5.45	**Smart Card Helper**	Not defined	
3.5.46	**SNMP Service**	Disabled	
3.5.47	**SNMP Trap**	Disabled	
3.5.48	**SQL Server Agent**	Not defined	Disable and uninstall the MS SQL server agent if it is not required.
3.5.49	**System Event Notification**	Not defined	
3.5.50	**Task Scheduler**	Not defined	Restrict Users and System access to the AT.EXE program.
3.5.51	**TCP/IP NetBIOS Helper Service**	Not defined	
3.5.52	**Telephony**	Not defined	
3.5.53	**Telnet**	Disabled	
3.5.54	**Uninterruptible Power Supply**	Not defined	
3.5.55	**Utility Manager**	Not defined	
3.5.56	**Windows Installer**	Not defined	
3.5.57	**Windows Management Instrumentation**	Not defined	
3.5.58	**Windows Management Instrumentation Driver Extensions**	Not defined	
3.5.59	**Windows Time**	Not defined	
3.5.60	**Workstation**	Not defined	
3.5.61	**World Wide Web Publishing Services**	Disabled	

B.3.6 File Permissions

Table B-11 defines the permissions for files and folders that can be found on Windows 2000 Professional. Please note that not all of these resources will be available on all installations of Windows 2000 Professional.

System Variable definitions
%systemroot% = C:\winnt
%systemdrive% = C:\

Table B-11. File Permission Settings

	File System	Policy	Owner	Security Permissions				
				Administrators	System	Creator Owner	Users	(Other)
3.6.1	**%ProgramFiles%**	Configure this file or folder; then, replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (this folder, subfolders, and files)	Full Control (this folder, subfolders, and files)	Full Control (subfolders and files only)	Read and Execute, List Folder Contents, Read (this folder, subfolders and files)	
3.6.2	**%SystemRoot%**	Configure this file or folder; then, replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (this folder, subfolders, and files)	Full Control (this folder, subfolders, and files)	Full Control (subfolders and files only)	Read and Execute, List Folder Contents, Read (this folder, subfolders and files)	
3.6.3	**%SystemRoot%\system32\appmgmt**	Configure this file or folder; then, propagate permissions to all subfolders and files	Administrators	Full Control (this folder, subfolders, and files)	Full Control (this folder, subfolders, and files)		Read and Execute, List Folder Contents, Read (this folder, subfolders and files)	
3.6.4	**%SystemRoot%\config**	Configure this file or folder; then, replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (this folder, subfolders, and files)	Full Control (this folder, subfolders, and files)			
3.6.5	**%SystemRoot%\system32\dllcache**	Configure this file or folder; then, replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (this folder, subfolders, and files)	Full Control (this folder, subfolders, and files)	Full Control (this folder, subfolders, and files)		
3.6.6	**%SystemRoot%\system32\DTCLog**	Configure this file or folder; then, replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (this folder, subfolders, and files)	Full Control (this folder, subfolders, and files)	Full Control (subfolders and files only)	Read and Execute, List Folder Contents, Read (this folder, subfolders and files)	

	File System	Policy	Owner	Security Permissions				
				Administrators	System	Creator Owner	Users	(Other)
3.6.7	**%SystemRoot%\system32\GroupPolicy**	Configure this file or folder; then, propagate permissions to all subfolders and files	Administrators	Full Control (this folder, subfolders, and files)	Full Control (this folder, subfolders, and files)			**Authenticated Users:** Read and Execute, List Folder Contents, Read (this folder, subfolders and files)
3.6.8	**%SystemRoot%\system32\ias**	Configure this file or folder; then, replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (this folder, subfolders, and files)	Full Control (this folder, subfolders, and files)	Full Control (this folder, subfolders, and files)		
3.6.9	**%SystemRoot%\system32\Ntbackup.exe**	Configure this file or folder; then, replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (this folder, subfolders, and files)	Full Control (this folder, subfolders, and files)			
3.6.10	**%SystemRoot%\system32\NTMSData**	Configure this file or folder; then, propagate permissions to all subfolders and files	Administrators	Full Control (this folder, subfolders, and files)	Full Control (this folder, subfolders, and files)			
3.6.11	**%SystemRoot%\system32\rcp.exe**	Configure this file or folder; then, replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (this folder, subfolders, and files)	Full Control (this folder, subfolders, and files)			
3.6.12	**%SystemRoot%\system32\regedt32.exe**	Configure this file or folder; then, replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (this folder, subfolders, and files)	Full Control (this folder, subfolders, and files)			
3.6.13	**%SystemRoot%\ReinstallBackups**	Do not allow permissions on this file or folder to be replaced	Administrators	Full Control (this folder, subfolders, and files)	Full Control (this folder, subfolders, and files)	Full Control (this folder, subfolders, and files)		**Power Users:** Read and Execute, List Folder Contents, Read (this folder, subfolders and files)
3.6.14	**%SystemRoot%\system32\rexec.exe**	Configure this file or folder; then, replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (this folder, subfolders, and files)	Full Control (this folder, subfolders, and files)			

	File System	Policy	Owner	Security Permissions				
				Administrators	System	Creator Owner	Users	(Other)
3.6.15	**SystemRoot%\system32\rsh.exe**	Configure this file or folder; then, replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (this folder, subfolders, and files)	Full Control (this folder, subfolders, and files)			
3.6.16	**%SystemRoot%\system32\secedit.exe**	Configure this file or folder; then, replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (this folder, subfolders, and files)	Full Control (this folder, subfolders, and files)			
3.6.17	**%SystemRoot%\system32\Setup**	Configure this file or folder; then, propagate permissions to all subfolders and files	Administrators	Full Control (this folder, subfolders, and files)	Full Control (this folder, subfolders, and files)		Read and Execute, List Folder Contents, Read (this folder, subfolders and files)	
3.6.18	**%SystemRoot%\system32\spool\printers**	Configure this file or folder; then, replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (this folder, subfolders, and files)	Full Control (this folder, subfolders, and files)	Full Control (subfolders and files only)	Traverse Folder/Execute File, Read attributes, Read extended attributes, Create folders/Append data (this folder and subfolders)	
3.6.19	**%SystemDrive%** ***Note:*** *This is going to generate a large amount of event log entries and may slow down the system.*	Configure this file or folder; then, propagate permissions to all subfolders and files	Administrators	Full Control (this folder, subfolders, and files)	Full Control (this folder, subfolders, and files)	Full Control (subfolders and files only)	Read and Execute, List Folder Contents, Read (this folder, subfolders and files)	**Enable Auditing – Everyone: Failure Full Control. Inherit to all files and folders.**
3.6.20	**%SystemDrive%\autoexec.bat**	Configure this file or folder; then, replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (this folder, subfolders, and files)	Full Control (this folder, subfolders, and files)			

	File System	Policy	Owner	Security Permissions				
				Administrators	System	Creator Owner	Users	(Other)
3.6.21	**%SystemDrive%\boot.ini**	Configure this file or folder; then, replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (this folder, subfolders, and files)	Full Control (this folder, subfolders, and files)			
3.6.22	**%SystemDrive%\config.sys**	Configure this file or folder; then, replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (this folder, subfolders, and files)	Full Control (this folder, subfolders, and files)			
3.6.23	**%SystemDrive%\Documents and Settings**	Configure this file or folder; then, propagate permissions to all subfolders and files	Administrators	Full Control (this folder, subfolders, and files)	Full Control (this folder, subfolders, and files)		Read and Execute, List Folder Contents, Read (this folder, subfolders and files)	
3.6.24	**%SystemDrive%\Documents and Settings\Administrator**	Configure this file or folder; then, replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (this folder, subfolders, and files)	Full Control (this folder, subfolders, and files)			
3.6.25	**%SystemDrive%\Documents and Settings\All Users**	Configure this file or folder; then, propagate permissions to all subfolders and files	Administrators	Full Control (this folder, subfolders, and files)	Full Control (this folder, subfolders, and files)		Read and Execute, List Folder Contents, Read (this folder, subfolders and files)	
3.6.26	**%SystemDrive%\Documents and Settings\Default User**	Configure this file or folder; then, replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (this folder, subfolders, and files)	Full Control (this folder, subfolders, and files)		Read and Execute, List Folder Contents, Read (this folder, subfolders and files)	

	File System	Policy	Owner	Security Permissions				
				Administrators	System	Creator Owner	Users	(Other)
3.6.27	**%SystemDrive%\ Documents and Settings\All Users\Documents \DrWatson**	Configure this file or folder; then, replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (this folder, subfolders, and files)	Full Control (this folder, subfolders, and files)	Full Control (subfolders and files only)	Traverse Folder/Execute File, List folder/Read data, Read attributes, Read extended attributes, Read permission(this folder, subfolders and files); Traverse Folder/Execute File, Create files/Write data, Create folders/Append data(subfolders and files only)	
3.6.28	**%SystemDrive%\I O.SYS**	Configure this file or folder; then, replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (this folder, subfolders, and files)	Full Control (this folder, subfolders, and files)			
3.6.29	**%SystemDrive%\ MSDOS.SYS**	Configure this file or folder; then, replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (this folder, subfolders, and files)	Full Control (this folder, subfolders, and files)			
3.6.30	**%SystemDrive%\n tdetect.com**	Configure this file or folder; then, replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (this folder, subfolders, and files)	Full Control (this folder, subfolders, and files)			
3.6.31	**%SystemDrive%\n tldr**	Configure this file or folder; then, replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (This folder only)	Full Control (This folder only)			
3.6.32	**%SystemDrive%\ Program Files\Resource Kit** *Note: this directory is present if the Resource Kit is installed*	Configure this file or folder; then, replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (this folder, subfolders, and files)	Full Control (this folder, subfolders, and files)			

	File System	Policy	Owner	Security Permissions				
				Administrators	System	Creator Owner	Users	(Other)
3.6.33	**%SystemDrive%\Temp** *Note: this directory is not present on a standard Windows installation. It is created and used by some third applications.*	Configure this file or folder; then, replace existing permissions on all subfolders and files with inheritable permissions ns	Administrators	Full Control (this folder, subfolders, and files)	Full Control (this folder, subfolders, and files)	Full Control (subfolders and files only)	Traverse Folder/Execute File, Create files/Write data, Create folders/Append data (this folder and subfolders)	
3.6.34	**%SystemRoot%\$NtServicePackUninstall$**	Configure this file or folder; then, replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (this folder, subfolders, and files)	Full Control (this folder, subfolders, and files)			
3.6.35	**%SystemRoot%\CSC**	Configure this file or folder; then, replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (this folder, subfolders, and files)	Full Control (this folder, subfolders, and files)			
3.6.36	**%SystemRoot%\debug**	Configure this file or folder; then, propagate permissions to all subfolders and files	Administrators	Full Control (this folder, subfolders, and files)	Full Control (this folder, subfolders, and files)	Full Control (subfolders and files only)	Read and Execute, List Folder Contents, Read (this folder, subfolders and files)	
3.6.37	**%SystemRoot%\Debug\UserMode**	Configure this file or folder; then, propagate permissions to all subfolders and files	Administrators	Full Control (this folder, subfolders, and files)	Full Control (this folder, subfolders, and files)		Traverse Folder/Execute File, List folder/Read data, Create files/Write data (this folder, only); Create files/Write data, Create folders/Append data (files only)	
3.6.38	**%SystemRoot%\Offline Web Pages**	Configure this file or folder; then, replace existing permissions on all subfolders and files with inheritable permissions	Administrators					**Everyone:** Full Control (this folder, subfolders, and files)

	File System	Policy	Owner	Security Permissions				
				Administrators	System	Creator Owner	Users	(Other)
3.6.39	**%SystemRoot%\regedit.exe**	Configure this file or folder; then, replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (this folder, subfolders, and files)	Full Control (this folder, subfolders, and files)			
3.6.40	**%SystemRoot%\Registration**	Configure this file or folder; then, propagate permissions to all subfolders and files	Administrators	Full Control (this folder, subfolders, and files)	Full Control (this folder, subfolders, and files)		Read (this folder, subfolders and files)	
3.6.41	**%SystemRoot%\repair**	Configure this file or folder; then, replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (this folder, subfolders, and files)	Full Control (this folder, subfolders, and files)			
3.6.42	**%SystemRoot%\security**	Configure this file or folder; then, replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (this folder, subfolders, and files)	Full Control (this folder, subfolders, and files)	Full Control (subfolders and files only)		
3.6.43	**%SystemRoot%\Tasks**	Configure this file or folder; then, replace existing permissions on all subfolders and files with inheritable permissions	Administrators					
3.6.44	**%SystemRoot%\Temp**	Configure this file or folder; then, replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (this folder, subfolders, and files)	Full Control (this folder, subfolders, and files)	Full Control (subfolders and files only)	Traverse Folder/Execute File, Create files/Write data, Create folders/Append data (this folder and subfolders)	
3.6.45	**c:\autoexec.bat**	Configure this file or folder; then, replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (this folder, subfolders, and files)	Full Control (this folder, subfolders, and files)			

	File System	Policy	Owner	Security Permissions				
				Administrators	System	Creator Owner	Users	(Other)
3.6.46	**c:\boot.ini**	Configure this file or folder; then, replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (this folder, subfolders, and files)	Full Control (this folder, subfolders, and files)			
3.6.47	**c:\config.sys**	Configure this file or folder; then, replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (this folder only)	Full Control (this folder only)			
3.6.48	**c:\ntbootdd.sys**	Configure this file or folder; then, replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (this folder only)	Full Control (this folder only)			
3.6.49	**c:\ntdetect.com**	Configure this file or folder; then, replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (this folder only)	Full Control (this folder only)			
3.6.50	**c:\ntldr**	Configure this file or folder; then, replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (this folder only)	Full Control (this folder only)			
3.6.51	**%SystemRoot%\at.exe**	Do not allow permissions on this file or folder to be replaced	Administrators	Full Control (this folder, subfolders, and files)				
3.6.52	**%SystemDrive%\ntbootdd.sys**	Configure this file or folder then Replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (This folder, subfolders and files)	Full Control (This folder only)			

	File System	Policy	Owner	Security Permissions				
				Administrators	System	Creator Owner	Users	(Other)
3.6.53	**%SystemRoot%\system32**	Configure this file or folder then Replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (This folder, subfolders and files)	Full Control (This folder, subfolders and files)	Full Control (Subfolders and files only)	Read and Execute, List Folder Contents, Read (This folder, subfolders and files)	
Netscape Communicator 4.7x file permission specific settings								
3.6.1N	**%SystemDrive%\Program Files\Netscape\Users**	Configure this file or folder then Replace existing permissions on all subfolders and files with inheritable permissions	Administrators				Modify, read and execute, list folder contents, read, write	Allow inheritable permissions from parent to propagate to this object
3.6.2N	**%SystemRoot%\nsreg.dat**	Configure this file or folder then Replace existing permissions on all subfolders and files with inheritable permissions	Administrators				Modify, read and execute, list folder contents, read, write	Allow inheritable permissions from parent to propagate to this object
The following executables are included in the NISTWin2kProGoldPlus.inf template								
3.6.1P	**%SystemRoot%\ServicePackFiles**	Configure this file or folder then Replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (This folder, subfolders and files)	Full Control (This folder, subfolders and files)			
3.6.2P	**%SystemRoot%\system32\arp.exe**	Configure this file or folder then Replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (This folder, subfolders and files)	Full Control (This folder, subfolders and files)			
3.6.3P	**%SystemRoot%\system32\cacls.exe**	Configure this file or folder then Replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (This folder, subfolders and files)	Full Control (This folder, subfolders and files)			
3.6.4P	**%SystemRoot%\system32\debug.exe**	Configure this file or folder then Replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (This folder, subfolders and files)	Full Control (This folder, subfolders and files)			

	File System	Policy	Owner	Security Permissions				
				Administrators	System	Creator Owner	Users	(Other)
3.6.5P	**%SystemRoot%\system32\edit.com**	Configure this file or folder then Replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (This folder, subfolders and files)	Full Control (This folder, subfolders and files)			
3.6.6P	**%SystemRoot%\system32\edlin.exe**	Configure this file or folder then Replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (This folder, subfolders and files)	Full Control (This folder, subfolders and files)			
3.6.7P	**%SystemRoot%\system32\finger.exe**	Configure this file or folder then Replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (This folder, subfolders and files)	Full Control (This folder, subfolders and files)			
3.6.8P	**%SystemRoot%\system32\ftp.exe**	Configure this file or folder then Replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (This folder, subfolders and files)	Full Control (This folder, subfolders and files)			
3.6.9P	**%SystemRoot%\system32\irftp.exe**	Configure this file or folder then Replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (This folder, subfolders and files)	Full Control (This folder, subfolders and files)			
3.6.10P	**%SystemRoot%\system32\tftp.exe**	Configure this file or folder then Replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (This folder, subfolders and files)	Full Control (This folder, subfolders and files)			
3.6.11P	**%SystemRoot%\system32\xcopy.exe**	Configure this file or folder then Replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (This folder, subfolders and files)	Full Control (This folder, subfolders and files)			
3.6.12P	**%SystemRoot%\system32\net.exe**	Configure this file or folder then Replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (This folder, subfolders and files)	Full Control (This folder, subfolders and files)			

	File System	Policy	Owner	Security Permissions				
				Administrators	System	Creator Owner	Users	(Other)
3.6.13P	**%SystemRoot%\system32\ipconfig.exe**	Configure this file or folder then Replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (This folder, subfolders and files)	Full Control (This folder, subfolders and files)			
3.6.14P	**%SystemRoot%\system32\nslookup.exe**	Configure this file or folder then Replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (This folder, subfolders and files)	Full Control (This folder, subfolders and files)			
3.6.15P	**%SystemRoot%\system32\telnet.exe**	Configure this file or folder then Replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (This folder, subfolders and files)	Full Control (This folder, subfolders and files)			
3.6.16P	**%SystemRoot%\system32\nbtstat.exe**	Configure this file or folder then Replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (This folder, subfolders and files)	Full Control (This folder, subfolders and files)			
3.6.17P	**%SystemRoot%\system32\ping.exe**	Configure this file or folder then Replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (This folder, subfolders and files)	Full Control (This folder, subfolders and files)			
3.6.18P	**%SystemRoot%\system32\pathping.exe**	Configure this file or folder then Replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (This folder, subfolders and files)	Full Control (This folder, subfolders and files)			
3.6.19P	**%SystemRoot%\system32\route.exe**	Configure this file or folder then Replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (This folder, subfolders and files)	Full Control (This folder, subfolders and files)			
3.6.20P	**%SystemRoot%\system32\runonce.exe**	Configure this file or folder then Replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (This folder, subfolders and files)	Full Control (This folder, subfolders and files)			

	File System	Policy	Owner	Security Permissions				
				Administrators	System	Creator Owner	Users	(Other)
3.6.21P	**%SystemRoot%\system32\ipxroute.exe**	Configure this file or folder then Replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (This folder, subfolders and files)	Full Control (This folder, subfolders and files)			
3.6.22P	**%SystemRoot%\system32\syskey.exe**	Configure this file or folder then Replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (This folder, subfolders and files)	Full Control (This folder, subfolders and files)			
3.6.23P	**%SystemRoot%\system32\tracert.exe**	Configure this file or folder then Replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (This folder, subfolders and files)	Full Control (This folder, subfolders and files)			
3.6.24P	**%SystemRoot%\system32\cmd.exe**	Configure this file or folder then Replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (This folder, subfolders and files)	Full Control (This folder, subfolders and files)			
3.6.25P	**%SystemRoot%\system32\cscript.exe**	Configure this file or folder then Replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (This folder, subfolders and files)	Full Control (This folder, subfolders and files)			
3.6.26P	**%SystemRoot%\system32\regsvr32.exe**	Configure this file or folder then Replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (This folder, subfolders and files)	Full Control (This folder, subfolders and files)			
3.6.27P	**%SystemRoot%\system32\runas.exe**	Configure this file or folder then Replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (This folder, subfolders and files)	Full Control (This folder, subfolders and files)			
3.6.28P	**%SystemRoot%\system32\netsh.exe**	Configure this file or folder then Replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (This folder, subfolders and files)	Full Control (This folder, subfolders and files)			

	File System	Policy	Owner	Security Permissions				
				Administrators	System	Creator Owner	Users	(Other)
3.6.29P	**%SystemRoot%\system32\wscript.exe**	Configure this file or folder then Replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (This folder, subfolders and files)	Full Control (This folder, subfolders and files)			
3.6.30P	**%SystemRoot%\system32\nwscript.exe**	Configure this file or folder then Replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (This folder, subfolders and files)	Full Control (This folder, subfolders and files)			
3.6.31P	**%SystemRoot%\system32\appmgmts.dll**	Configure this file or folder then Replace existing permissions on all subfolders and files with inheritable permissions	Administrators	Full Control (This folder, subfolders and files)	Full Control (This folder, subfolders and files)			

B.3.7 Registry Keys Modifications

Table B-12 lists the registry keys modifications made by the NIST template.

Table B-12. Registry Keys Settings

	Registry Keys	Policy	Owner	Security Permissions				
				Administrators	System	Creator Owner	Users	(Other)
3.7.1	**CLASSES_ROOT**	Configure this key then Replace existing permissions on all subkeys with inheritable permissions	Administrators	Full Control (this key and subkeys)	Full Control (this key and subkeys)	Full Control (subkeys only)	Read and Execute (this key and subkeys)	
3.7.2	**MACHINE\SOFTWARE** ***Note:*** *This is going to generate a large amount of event log entries and may slow down the system.*	Configure this key then Replace existing permissions on all subkeys with inheritable permissions	Administrators	Full Control (this key and subkeys)	Full Control (this key and subkeys)	Full Control (subkeys only)	Read and Execute (this key and subkeys)	**Audit: Everyone: Failure Full Control(this key and subkeys)**

	Registry Keys	Policy	Owner	Security Permissions				
				Administrators	System	Creator Owner	Users	(Other)
3.7.3	**MACHINE\SOFTWARE\Microsoft\NetDDE**	Configure this key then Replace existing permissions on all subkeys with inheritable permissions	Administrators	Full Control (this key and subkeys)	Full Control (this key and subkeys)			
3.7.4	**MACHINE\SOFTWARE\Microsoft\OS/2 Subsystem for NT**	Configure this key then Replace existing permissions on all subkeys with inheritable permissions	Administrators	Full Control (this key and subkeys)	Full Control (this key and subkeys)	Full Control (subkeys only)		
3.7.5	**MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AsrCommands**	Configure this key then Replace existing permissions on all subkeys with inheritable permissions	Administrators	Full Control (this key and subkeys)	Full Control (this key and subkeys)	Full Control (subkeys only)	Read and Execute (this key and subkeys)	**Backup Operators:** Query Value, Set Value, Create Subkey, Enumerate Subkeys, Notify, Delete, Read permissions (this key and subkeys)
3.7.6	**MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib**	Configure this key then Replace existing permissions on all subkeys with inheritable permissions	Administrators	Full Control (this key and subkeys)	Full Control (this key and subkeys)	Full Control (this key and subkeys)		**INTERACTIVE:** Read (this key and subkeys)
3.7.7	**MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy**	Configure this key then Propagate heritable permissions to all subkeys	Administrators	Full Control (this key and subkeys)	Full Control (this key and subkeys)			**Authenticated Users:** Read and Execute (this key and subkeys)
3.7.8	**MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer**	Configure this key then Propagate heritable permissions to all subkeys	Administrators	Full Control (this key and subkeys)	Full Control (this key and subkeys)		Read and Execute (this key and subkeys)	
3.7.9	**MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies**	Configure this key then Propagate heritable permissions to all subkeys	Administrators	Full Control (this key and subkeys)	Full Control (this key and subkeys)			**Authenticated Users:** Read and Execute (this key and subkeys)
3.7.10	**MACHINE\SYSTEM** ***Note:*** *This is going to generate a large amount of event log entries and may slow down the system.*	Configure this key then Replace existing permissions on all subkeys with inheritable permissions	Administrators	Full Control (this key and subkeys)	Full Control (this key and subkeys)	Full Control (subkeys only)	Read and Execute (this key and subkeys)	**Audit: Everyone: Failure Full Control(this key and subkeys)**

	Registry Keys	Policy	Owner	Security Permissions				
				Administrators	System	Creator Owner	Users	(Other)
3.7.11	MACHINE\SYSTEM\Clone	Do not allow permissions on this key to be replaced	Administrators					Allow inheritable permissions from parent to propagate to this object
3.7.12	MACHINE\SYSTEM\ControlSet001	Configure this key then Propagate heritable permissions to all subkeys	Administrators	Full Control (this key and subkeys)	Full Control (this key and subkeys)	Full Control (subkeys only)	Read and Execute (this key and subkeys)	
3.7.13	MACHINE\SYSTEM\ControlSet002	Configure this key then Propagate heritable permissions to all subkeys	Administrators	Full Control (this key and subkeys)	Full Control (this key and subkeys)	Full Control (subkeys only)	Read and Execute (this key and subkeys)	
3.7.14	MACHINE\SYSTEM\ControlSet003	Configure this key then Propagate heritable permissions to all subkeys	Administrators	Full Control (this key and subkeys)	Full Control (this key and subkeys)	Full Control (subkeys only)	Read and Execute (this key and subkeys)	
3.7.15	MACHINE\SYSTEM\ControlSet004	Configure this key then Propagate heritable permissions to all subkeys	Administrators	Full Control (this key and subkeys)	Full Control (this key and subkeys)	Full Control (subkeys only)	Read and Execute (this key and subkeys)	
3.7.16	MACHINE\SYSTEM\ControlSet005	Configure this key then Propagate heritable permissions to all subkeys	Administrators	Full Control (this key and subkeys)	Full Control (this key and subkeys)	Full Control (subkeys only)	Read and Execute (this key and subkeys)	
3.7.17	MACHINE\SYSTEM\ControlSet006	Configure this key then Propagate heritable permissions to all subkeys	Administrators	Full Control (this key and subkeys)	Full Control (this key and subkeys)	Full Control (subkeys only)	Read and Execute (this key and subkeys)	
3.7.18	MACHINE\SYSTEM\ControlSet007	Configure this key then Propagate heritable permissions to all subkeys	Administrators	Full Control (this key and subkeys)	Full Control (this key and subkeys)	Full Control (subkeys only)	Read and Execute (this key and subkeys)	
3.7.19	MACHINE\SYSTEM\ControlSet008	Configure this key then Propagate heritable permissions to all subkeys	Administrators	Full Control (this key and subkeys)	Full Control (this key and subkeys)	Full Control (subkeys only)	Read and Execute (this key and subkeys)	
3.7.20	MACHINE\SYSTEM\ControlSet009	Configure this key then Propagate heritable permissions to all subkeys	Administrators	Full Control (this key and subkeys)	Full Control (this key and subkeys)	Full Control (subkeys only)	Read and Execute (this key and subkeys)	
3.7.21	MACHINE\SYSTEM\ControlSet010	Configure this key then Propagate heritable permissions to all subkeys	Administrators	Full Control (this key and subkeys)	Full Control (this key and subkeys)	Full Control (subkeys only)	Read and Execute (this key and subkeys)	

	Registry Keys	Policy	Owner	Security Permissions				
				Administrators	System	Creator Owner	Users	(Other)
3.7.22	**MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg**	Configure this key then Replace existing permissions on all subkeys with inheritable permissions	Administrators	Full Control (this key and subkeys)	Full Control (this key and subkeys)			**Backup Operators:** Query Value, Enumerate Subkeys, Notify, Read permissions (this key only)
3.7.23	**MACHINE\SYSTEM\CurrentControlSet\Control\WMI\Security**	Configure this key then Replace existing permissions on all subkeys with inheritable permissions	Administrators	Full Control (This key and subkeys)	Full Control (this key and subkeys)	Full Control (this key and subkeys)		
3.7.24	**MACHINE\SYSTEM\CurrentControlSet\Enum**	Do not allow permissions on this key to be replaced	Administrators	Full Control (this key and subkeys)	Full Control (this key and subkeys)			**Authenticated Users:** Read and Execute (this key and subkeys)
3.7.25	**MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles**	Configure this key then Propagate heritable permissions to all subkeys	Administrators	Full Control (this key and subkeys)	Full Control (this key and subkeys)	Full Control (subkeys only)	Read and Execute (this key and subkeys)	
3.7.26	**MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\PermittedManagers**	Configure this key then Replace existing permissions on all subkeys with inheritable permissions	Administrators	Full Control (this key and subkeys)	Full Control (this key and subkeys)	Full Control (subkeys only)		
3.7.27	**MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ValidCommunities**	Configure this key then Replace existing permissions on all subkeys with inheritable permissions	Administrators	Full Control (this key and subkeys)	Full Control (this key and subkeys)	Full Control (subkeys only)		
3.7.28	**USERS\.DEFAULT**	Configure this key then Replace existing permissions on all subkeys with inheritable permissions	Administrators	Full Control (this key and subkeys)	Full Control (this key and subkeys)	Full Control (subkeys only)	Read and Execute (this key and subkeys)	
3.7.29	**USERS\.DEFAULT\Software\Microsoft\NetDDE**	Configure this key then Replace existing permissions on all subkeys with inheritable permissions	Administrators	Full Control (this key and subkeys)	Full Control (this key and subkeys)			
3.7.30	**USERS\.DEFAULT\SOFTWARE\Microsoft\Protected Storage System Provider**	Do not allow permissions on this key to be replaced	Administrators					

	Registry Keys	Policy	Owner	Security Permissions				
				Administrators	System	Creator Owner	Users	(Other)
3.7.31	MACHINE\SOFTWARE\Microsoft\protected storage provider	Do not allow permissions on this key to be replaced	Administrators					Allow inheritable permissions from parent to propagate to this object
Netscape Communicator registry specific settings								
3.7.1N	CLASSES_ROOT\CLSID\{EF5F7050-385A-11CE-8193-0020AF18F905}	Configure this key then Replace existing permissions on all subkeys with inheritable permissions					Read, execute, write, delete	Allow inheritable permissions from parent to propagate to this object
3.7.2N	CLASSES_ROOT\CLSID\{E67D6A10-4438-11CE-8CE4-0020AF18F905}	Configure this key then Replace existing permissions on all subkeys with inheritable permissions					Read, execute, write, delete	Allow inheritable permissions from parent to propagate to this object
3.7.3N	CLASSES_ROOT\CLSID\{E328732C-9DC9-11CF-92D0-004095E27A10}	Configure this key then Replace existing permissions on all subkeys with inheritable permissions					Read, execute, write, delete	Allow inheritable permissions from parent to propagate to this object
3.7.4N	CLASSES_ROOT\CLSID\{61D8DE20-CA9A-11CE-9EA5-0080C82BE3B6}	Configure this key then Replace existing permissions on all subkeys with inheritable permissions					Read, execute, write, delete	Allow inheritable permissions from parent to propagate to this object
3.7.5N	CLASSES_ROOT\CLSID\{60403D81-872B-11CF-ACC8-0080C82BE3B6}	Configure this key then Replace existing permissions on all subkeys with inheritable permissions					Read, execute, write, delete	Allow inheritable permissions from parent to propagate to this object
3.7.6N	CLASSES_ROOT\CLSID\{481ED670-9D30-11ce-8F9B-0800091AC64E}	Configure this key then Replace existing permissions on all subkeys with inheritable permissions					Read, execute, write, delete	Allow inheritable permissions from parent to propagate to this object
3.7.7N	CLASSES_ROOT\aimfile",2," D:AR(A;CI;CCDCLCSWRPSDRC;;;BU)	Configure this key then Replace existing permissions on all subkeys with inheritable permissions					Read, execute, write, delete	Allow inheritable permissions from parent to propagate to this object
3.7.8N	MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\Netscape.exe	Configure this key then Replace existing permissions on all subkeys with inheritable permissions					Read, execute, write, delete	Allow inheritable permissions from parent to propagate to this object

	Registry Keys	Policy	Owner	Security Permissions				
				Administrators	System	Creator Owner	Users	(Other)
3.7.9N	MACHINE\SOFTWARE\Netscape\Netscape Navigator	Configure this key then Replace existing permissions on all subkeys with inheritable permissions					Read, execute, write, delete	Allow inheritable permissions from parent to propagate to this object
3.7.10N	CLASSES_ROOT\Netscape Markup	Configure this key then Replace existing permissions on all subkeys with inheritable permissions					Read, execute, write, delete	Allow inheritable permissions from parent to propagate to this object
3.7.11N	CLASSES_ROOT\Netscape.Registry.1\CLSID	Configure this key then Replace existing permissions on all subkeys with inheritable permissions					Read, execute, write, delete	Allow inheritable permissions from parent to propagate to this object
3.7.12N	CLASSES_ROOT\Netscape.TalkNav.1\CLSID	Configure this key then Replace existing permissions on all subkeys with inheritable permissions					Read, execute, write, delete	Allow inheritable permissions from parent to propagate to this object
3.7.13N	CLASSES_ROOT\Netscape.Help.1\CLSID	Configure this key then Replace existing permissions on all subkeys with inheritable permissions					Read, execute, write, delete	Allow inheritable permissions from parent to propagate to this object
3.7.14N	CLASSES_ROOT\Netscape.Network.1\CLSID	Configure this key then Replace existing permissions on all subkeys with inheritable permissions					Read, execute, write, delete	Allow inheritable permissions from parent to propagate to this object
3.7.15N	CLASSES_ROOT\Netscape Markup\CLSID	Configure this key then Replace existing permissions on all subkeys with inheritable permissions					Read, execute, write, delete	Allow inheritable permissions from parent to propagate to this object

B.3.8 Registry Values

Table B-13 lists the registry values that are defined in the NIST template.

Table B-13. Registry Values

	Registry Value Name and Path	Data Type	Data Value
3.8.1	MACHINE\SOFTWARE\Microsoft\Command Processor\PathCompletionChar ***Note:*** *To enable path completion, set this value to 9 to map it to the tab key.*	REG_DWORD	Not Defined
3.8.2	MACHINE\SOFTWARE\Microsoft\DrWatson\CreateCrashDump	REG_DWORD	0
3.8.3	MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\AutoAdminLogon	REG_SZ	0
3.8.4	MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SFCDisable ***Note:*** *If the Windows File Protection/System File Checker is enabled, set this value to 4 to enabled, with popups disabled.*	REG_DWORD	Not defined
3.8.5	MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug\Auto	REG_DWORD	0
3.8.6	MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\DontDisplayLastUserName	REG_SZ	1
3.8.7	MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SFCScan ***Note:*** *If the Windows File Protection/System File Checker is enabled, set this value to 1 to scan protected files at every boot.*	REG_DWORD	Not defined
3.8.8	MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SFCShowProgress ***Note:*** *If the Windows File Protection/System File Checker is enabled, set this value to 0 to hide the System File Checker progress meter.*	REG_DWORD	Not defined
3.8.9	MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Network\NoDialIn	REG_DWORD	1
3.8.10	MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Network\HideSharePwds	REG_DWORD	1
3.8.11	MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun	REG_DWORD	255
3.8.12	MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl\AutoReboot	REG_DWORD	0
3.8.13	MACHINE\SYSTEM\CurrentControlSet\Services\MrxSmb\Parameters\RefuseReset	REG_DWORD	1
3.8.14	MACHINE\SYSTEM\CurrentControlSet\Services\Cdrom\Autorun	REG_DWORD	0
3.8.15	MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\AutoShareWks *Note: This may break some network management tools that expect to be able to access the drives on a workstation remotely.*	REG_DWORD	0
3.8.16	MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters\NoNameReleaseOnDemand	REG_DWORD	1
3.8.17	MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\PerformRouterDiscovery	REG_DWORD	0
3.8.18	MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect	REG_DWORD	2
3.8.19	MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxHalfOpen	REG_DWORD	100
3.8.20	MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxHalfOpenRetried	REG_DWORD	80

	Registry Value Name and Path	Data Type	Data Value
3.8.21	MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSourceRouting	REG_DWORD	2
3.8.22	MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTime	REG_DWORD	300000
3.8.23	MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableDeadGWDetect	REG_DWORD	0
3.8.24	MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirect	REG_DWORD	0
3.8.25	MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnablePMTUDiscovery	REG_DWORD	1
3.8.26	MACHINE\SYSTEM\CurrentControlSet\Services\IPSEC\NoDefaultExempt *Note: This will break Kerberos authentication with IPSec. Add specific rules allowing Kerberos TCP/UDP 88 if they do not already exist*	REG_DWORD	1
3.8.27	MACHINE\SYSTEM\CurrentControlCet\Services\Lanmanserver\Parameters\Hidden	REG_DWORD	1
3.8.28	USERS\.DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun	REG_DWORD	255

Appendix C—Tools

Appendix C summarizes the various tools that can be used to configure, manage, and monitor the security Windows 2000 Professional settings.

Tool Name	Description	Reference
mmc.exe	Microsoft Management Console. It is the container for snap-ins.	Included with Windows 2000 systems
Security Configuration and Analysis MMC snap-in	Used to apply, review, and modify security templates.	Included with Windows 2000 systems
Local Security Policy	Allows modification of local workstation policy settings.	Included with Windows 2000 systems
Regedt32.exe	An interface used to modify windows registry settings.	Included with Windows 2000 systems
Secedit.exe	Command line interface used to apply security templates.	Included with Windows 2000 systems
Cacls.exe	Command line interface used to display and modify ACLs of files.	Included with Windows 2000 systems
Hfnetchk.exe	Command line tool to allow SAs to centrally check Microsoft computers for the absence of patches.	This program can be downloaded from Microsoft at http://support.microsoft.com/default.aspx?scid=kb;EN-US;q303215
Qchain.exe	Allows SAs to apply multiple hotfixes to a machine without rebooting between each hotfix.	This program can be downloaded from Microsoft at http://support.microsoft.com/default.aspx?scid=kb;EN-US;q296861
RegSnap	Tool compares before and after "snapshots" of the registry.	This tool can be purchased from LastBit software at http://www.webdon.com/regsnap/default.asp
MBSA	Microsoft Baseline Security Advisor (MBSA), an ActiveX security control vulnerability scanner.	The MBSA generates a report of necessary fixes to address in order of criticality. It is found at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/Tools/MBSAhome.asp
Qfecheck.exe	Command line tool to verify installed hotfixes	This program can be downloaded from Microsoft at http://support.microsoft.com/default.aspx?scid=kb;en-us;Q282784
ICAT	***ICAT*** is a searchable index of information on computer vulnerabilities. It provides search capability at a fine granularity and links users to vulnerability and patch information.	http://icat.nist.gov/icat.cfm

CIS Windows 2000 Professional Operating System Benchmark - Consensus Baseline Security Settings	Security configuration recommendations beyond the minimum due care level for Windows 2000 workstations. This Benchmark reflects the content of the Consensus Baseline Security Settings document developed by the Members of The Center for Internet Security (CIS), The SANS Institute, and the following agencies of the United States federal government: The National Security Agency (NSA), The Defense Information Systems Agency (DISA), The National Institute of Standards and Technology (NIST), and The General Services Administration (GSA).	http://www.cisecurity.org/bench_win2000.html

Appendix D—Windows XP Security Components Overview

Appendix D focuses on the networking changes and potential security improvements to Windows 2000 Professional provided by the latest member of the Windows family of operating systems, Windows XP. The following text is provided for informational purposes only. The benefits listed within this Appendix have neither been fully tested nor verified.

D.1 Windows XP Background

Windows XP (XP), originally code-named Whistler, is sold in three distinct versions: one for consumers, one for the majority of commercial establishments, and one for organizations that run Intel's 64-bit Itanium family of processors. All available versions of Windows XP are built around the core Windows 2000 kernel and are fully compatible while deployed within a Windows 2000 environment. Microsoft's Windows XP home page is located at the following URL: http://www.microsoft.com/windowsxp/

D.2 Bridging

XP has made some changes to networking support over Windows 2000 Professional. One new networking feature of XP is called a bridge. A bridge allows two or more networks to be connected in such a way that they act like a single network. This bridging is not limited to any one type of network connection; at its release, XP will support network bridging with Ethernet, Wireless Ethernet (802.11x), and Firewire Institute of Electrical and Electronic Engineers (IEEE) 1394 networks. Bridging allows these two networks to act as a single network with a single Internet Protocol (IP) schema. The security implications of this feature remain to be seen.

D.3 Wireless Ethernet Protocol

Another significant advancement in XP networking is the default support for the Wireless Ethernet protocol (802.1x). Windows 2000 Professional users need to install additional software to provide this same support. Windows XP provides as a default better wireless performance and security over other Windows platforms. Because 802.1x uses IP for communications, it can rely on IP systems services in the OS. Wireless network support within Windows XP offers the following features:

- Improved performance over Windows 2000 Professional, with TCP optimizations for the unique requirements of wireless communications
- Seamless routing, which automatically detects not only a move to a new access point, forcing reauthentication to ensure appropriate network access but also changes in the IP subnet so an appropriate address can be used to get optimum resource access
- Enhanced quality of service (QoS) support
- Automatic network detection and configuration
- Secure access to resources in the network, protected by Windows Login.

The NIST Special Publication 800-48, Wireless Network Security: 802.11, Bluetoth, and Handheld Devices, describes in detail the security issues that apply to Wireless Network. http://csrc.nist.gov/publications/

D.4 Remote Assistance

Remote Assistance features are a new addition to XP. Remote Assistance offers services similar to those provided by software titles such as Virtual Network Computing (VNC) and enables users to share control of their XP computer with other XP computers. This feature can be centrally or locally enabled or disabled. Remote Assistance, like all other remote control software, should be considered a high-risk service.

D.5 Remote Desktop Services

XP also offers Remote Desktop services powered by the Remote Desktop Protocol 5.0 (RDP). The Remote Desktop services are designed to allow users to gain access to network resources, data, and applications located on their computer from a remote location. This closely resembles Windows Terminal Services. RDP is designed to function even in limited bandwidth because only keyboard, mouse and display signals are transmitted over the network. Hosting is not available with Windows XP Home Edition. Remote Desktop can be enabled or disabled. The RDP service should be considered high risk in its default configuration.

Remote Desktop, shown in Figure D-1, has the following features:

- **File System Redirection.** This feature makes the local file system available on the remote desktop within a terminal session.
- **Printer Redirection.** This feature routes printing jobs from the terminal server to a printer attached to the local computer.
- **Port Redirection.** This feature enables applications running within a terminal session to have access to the serial and parallel ports on the client.
- **Audio.** This feature enables the user to run an audio-enabled application on a remote desktop and hear the audio output from speakers attached to the computer on which the work is being done.
- **Clipboard.** The Remote Desktop and the client computer share a clipboard that allows data to be interchanged.

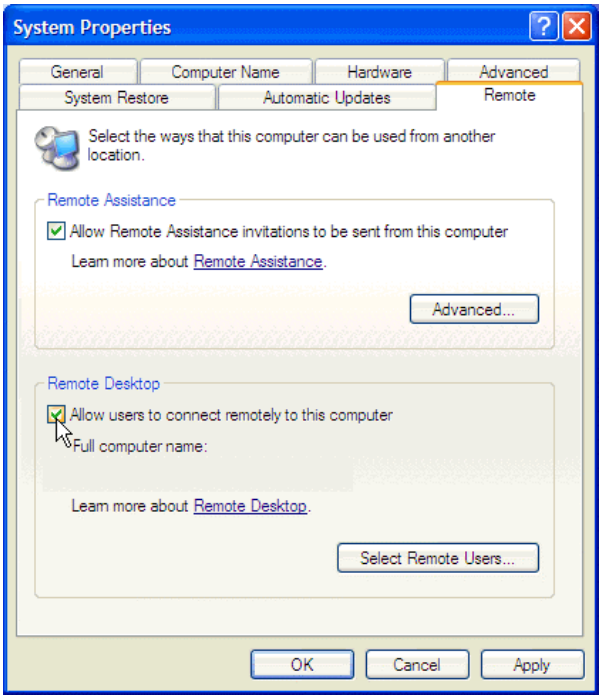

Figure D-1. XP Remote Desktop

D.6 Encrypted File System

Encrypted File System (EFS) improvements within XP include an ability to allow multiple users access to an encrypted document. In the Windows 2000 Professional implementation of EFS, only one user had access to a file encrypted with EFS. This additional feature allows the encryption of files for groups of individuals, allowing sensitive files needed by more than one person to be protected by more than just NTFS access control lists (ACL). EFS can be enabled for entire files or folders. Figure D-2 shows the XP EFS Enable Folder Attribute.

EFS can use either the expanded Data Encryption Standard (DESX) or the Triple–DES (3DES) as the encryption algorithm. Both the RSA Base and RSA Enhanced software that cryptographic service providers (CSP) included in the OS may be used for EFS certificates and for encryption of the symmetric encryption keys. By default, XP does not require a recovery agent to enable EFS. If a user leaves a company, no one can gain access to encrypted files—even an administrator on the local system. With Windows 2000 Server, administrators can set a policy to recover encrypted data if passwords are lost.

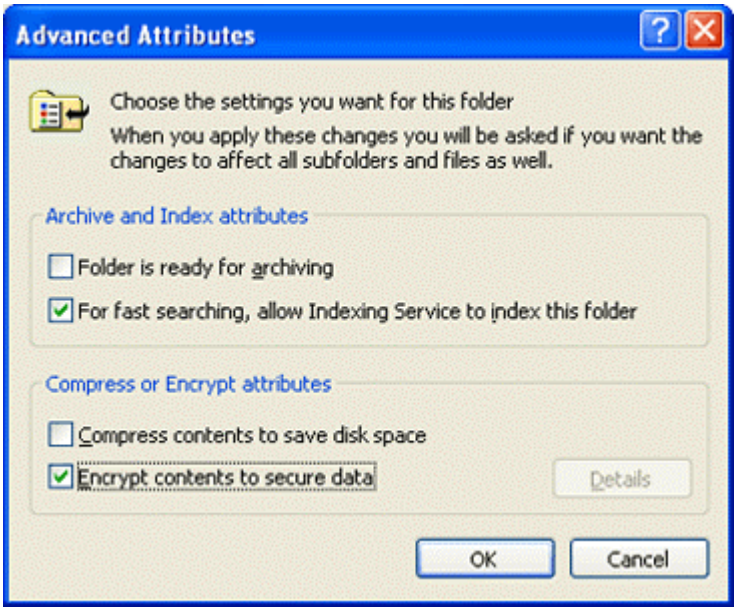

Figure D-2. XP EFS Enable Folder Attribute

EFS for XP also works with Offline Folders, shown in Figure D-3, by encrypting the entire offline files database to protect files used in offline browsing.

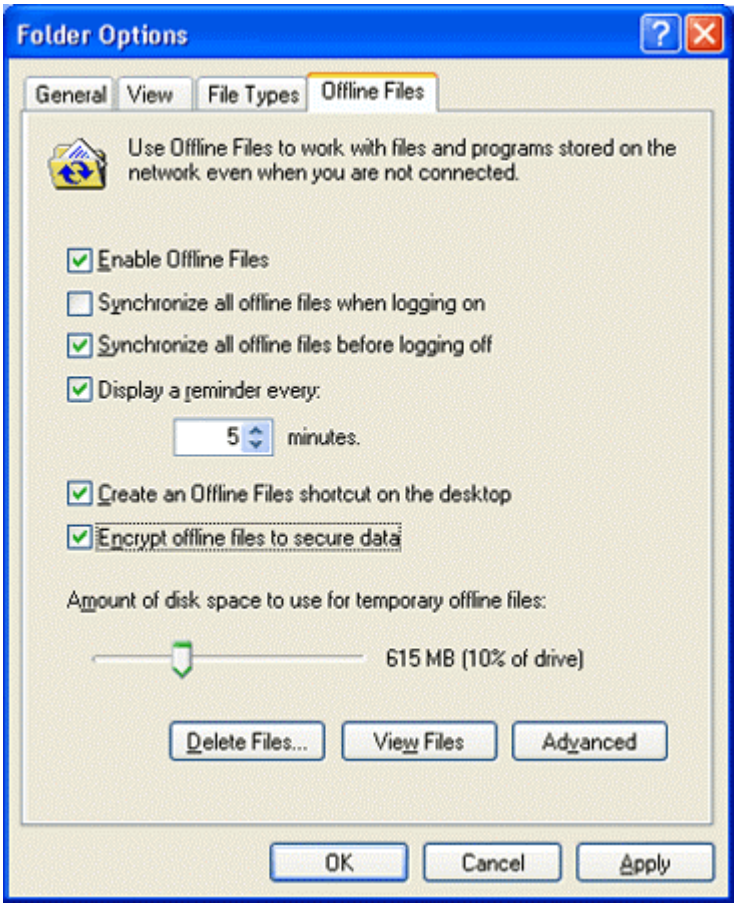

Figure D-3. EFS Enabled for Offline Files

D.7 Smart Card Support

XP has extended Windows 2000 Professional smart card support. When coupled with the Remote Desktop technology, a client can perform smart card operations on the remote machine.
In addition, smart card access can be specifically tied to tools and utilities. This feature allows SAs to use alternate credentials so they can conduct their normal business with normal user privileges, while simultaneously carrying out administrator functions without having to log in as an Administrative user. Utilities such as Net.exe and Runas.exe in Windows XP Professional have been enabled to support smart card credentials.

D.8 Network Logon

Remote connections into an XP machine are limited to Guest Level privileges by default. If an unauthorized user guesses the password to an XP machine remotely, the user will have only guest-level access to XP resources.

To protect users with nonpassword protected accounts, Windows XP Professional accounts without passwords can be used to log on only at the physical computer console. By default, accounts with blank passwords can no longer be used to log on to the computer remotely over the network or for any other logon activity except at the main physical console logon screen. For example, the user cannot use the secondary logon service (RunAs) to start a program as a local user with a blank password.

Note: This restriction applies to neither domain accounts nor local guest accounts. If a guest account is enabled and has a blank password, it will be permitted to log on and access any resource authorized for access by the guest account.

D.9 Integrated Firewall

Windows XP includes the Internet Connection Firewall (ICF), which is enabled by default during installation of Windows XP. Figure D-4 shows an XP ICF Enable screen. The ICF is packet inspection software that dynamically opens ports on the firewall for as long as needed to enable access to the services requested. By default, inbound ports are blocked; ICF uses port mapping and allows users to open holes in the firewall for inbound services to connect to if required. The ICF does not restrict outbound connections by default. ICF can be used on any IP-based connection, but it is specifically designed for home-based broadband connections.

Note: Most third-party firewalls restrict inbound connections and application or port-based outbound connections. Restricting of outbound connections increases the user's system security and reduces the potential damage it can inflict on other systems if compromised.

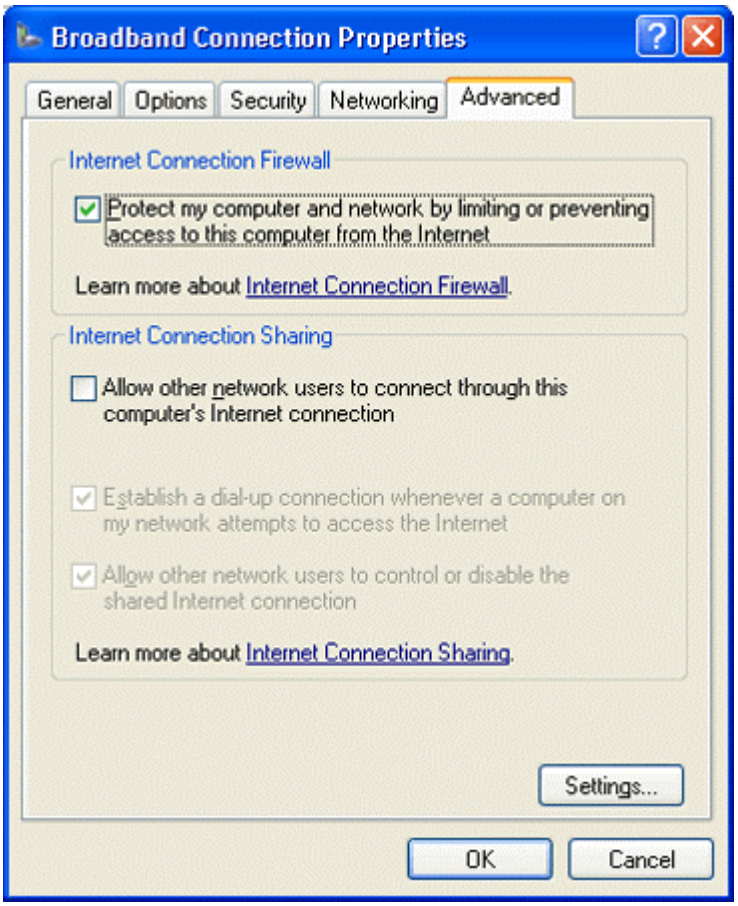

Figure D-4. XP ICF Enable Screen

D.10 Software Restriction Policy

Software restriction policies provide a policy-driven mechanism that identifies software running within a computer or domain and controls the ability of that software to execute. Using a software restriction policy, unwanted applications can be prevented from running. This can allow an Administrator full control over the applications that run within an environment and can help to prevent Trojan horse applications from running. An example of the Local Security Settings policy editor is shown in Figure D-5.

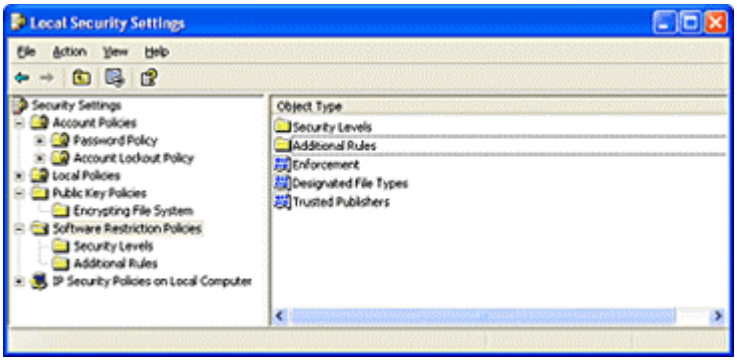

Figure D-5. XP Software Restrictions Policy

Software can be identified through one of the following rules:

- **Hash rule.** A software restriction policy's MMC snap-in allows an SA to browse to a file and identify that program by calculating its hash. A hash is a digital fingerprint that uniquely identifies a program or file.
- **Path rule.** A path rule can identify software by a full path name.
- **Certificate rule.** A certificate rule identifies software by the publisher certificate used to digitally sign the software.
- **Zone rule.** A zone rule identifies software that comes from the Internet, local intranet, trusted sites, or restricted sites zones.

Appendix E—References Used

Table E-1 presents the Internet references used in creating of this document. The documents listed are excellent resources to use for learning about Windows 2000 security.

Table E-1. References Used in Creating of this Document

Hyperlink URL and Description
http://nsa2.www.conxion.com/win2k/ Conxion has provided a high-speed mirror of Windows 2000 Security guidelines from NSA.
http://www.win2000mag.com/Articles/Index.cfm?ArticleID=15901&Key=Windows%202000%20Professional Article discussing antivirus solutions within Windows 2000.
http://www.windowsitsecurity.com/Articles/Index.cfm?ArticleID=15741 Article discussing EFS and implementing to secure an install of Windows 2000 on a portable computer.
http://www.windowsitsecurity.com/Articles/Index.cfm?ArticleID=15819 Article discussing Protecting Data Recovery Certificates in EFS.
http://support.microsoft.com/directory/article.asp?ID=KB;EN-US;Q230520 Microsoft Knowledge base article describing how to encrypt data using the Encrypting File System (EFS) in Windows 2000.
http://www.microsoft.com/windows2000/techinfo/planning/security/efssteps.asp A Windows 2000 feature step guide to implementing EFS. This is a part of the Microsoft Windows 2000 home page.
http://www.swynk.com/windows/efs.asp Additional article on EFS from swynk.com. Contains instructions on implementing EFS.
http://www-project.slac.stanford.edu/windows2000/updates/efs1.htm Stanford discussion on EFS as part of its infrastructure updates.

Hyperlink URL and Description
http://www.labmice.net/Windows2000/FileMgmt/EFS.htm Labmice.net resources on EFS within Windows 2000. This is an additional list of links to articles and documents written on EFS.
http://service1.symantec.com/SUPPORT/tsgeninfo.nsf/docid/199762382617 Article from Symantec Knowledge Base about creating ERD and how to use it to back up Windows 2000 registry.
http://www.jsiinc.com/SUBF/Tip2500/rh2532.htm Tip instructing how to create an ERD using Windows Scripting Host (WSH) and JScript.
http://is-it-true.org/nt/nt2000/atips/atips32.shtml Usage instructions for creating ERD using Recovery Console within Windows 2000
http://www.win2000mag.com/Articles/Index.cfm?ArticleID=22415&Key=Windows%202000%20Professional Article discussing IE 6 features and bugs.
http://www.win2000mag.com/Articles/Index.cfm?ArticleID=22347&Key=Windows%202000%20Professional Article from win2000mag.com discussing a technology new to the upcoming Windows XP, the Windows Client Update, and how IE 6 plays into the mix.
http://www.microsoft.com/windows/ie/evaluation/overview/default.asp From IE 6 Microsoft home page. This is an excellent site to learn more about the technologies specific to IE 6 under the hood.
http://search.microsoft.com/us/SearchMS25.asp?so=RECCNT&qu=Windows%202000%20professional%20security&boolean=ALL&i=00&i=01&i=02&i=03&i=04&i=05&i=06&i=07&i=08&i=09&p=1&nq=NEXT&fqu=*security%26%22windows%202000%20professional%22 Results of a search for the keywords “Microsoft Windows 2000 professional security” from the Microsoft.com search engine.
http://www.microsoft.com/office/ork/2000/journ/KioskMode.htm Microsoft.com site for installing Microsoft Office in a public environment. This article discusses privacy issues.

Hyperlink URL and Description
http://support.microsoft.com/support/kb/articles/Q249/3/45.ASP Microsoft.com knowledge base article on how to secure an install of Microsoft Office on Windows 2000.
http://www.win2000mag.com/Articles/Index.cfm?ArticleID=21577&Key=Windows%202000%20Professional Article discussing XP product activation codes, which is a new security feature of Office XP.
http://www.win2000mag.com/Articles/Index.cfm?ArticleID=20754&Key=Windows%202000%20Professional Article discussing pros and cons of upgrading to Office XP.
http://www.win2000mag.com/Articles/Index.cfm?ArticleID=21285&Key=Windows%202000%20Professional Article discussing the nuances of Office XP.
http://support.microsoft.com/directory/article.asp?ID=KB;EN-US;Q258289 Microsoft.com knowledge base article discussing the role of passwords in authentication process of Windows 2000.
http://www.win2000mag.com/Articles/Index.cfm?ArticleID=16215&Key=Windows%202000%20Professional Article discussing registry tips for Windows 2000 professional. These types of articles are actually hard to come by.
http://www.windowsitlibrary.com/Content/267/2.html Article discussing secedit.exe binary and how to manipulate and backup registry keys and hives.
http://archives.neohapsis.com/archives/sf/ms/2001-q3/0003.html Message archive describing a problem with importing homemade security templates with secedit.exe
http://www.sans.org/infosecFAQ/win2000/tools.htm SANS overview of security tools within Windows 2000.

Hyperlink URL and Description
http://www.sans.org/infosecFAQ/win/settings.htm SANS discussion about the secedit.exe binary and security template files.
http://www.shs.ilstu.edu/Windows2000/documents/installation_tools.htm Document intended to be a resource for SAs migrating legacy Windows machines to Windows 2000; contains information regarding secedit.exe.
http://www.activewin.com/tips/win2000/1/2000_tips_4.shtml Tips and tricks from activewin.com for use of secedit.exe especially to validate a security template.
http://www.win2000mag.com/Articles/Index.cfm?ArticleID=20517&Key=Windows%202000%20Professional Article regarding upgrade possibilities and requirements to upgrade your Windows 2000 client to Windows XP.
http://www.win2000mag.com/Articles/Index.cfm?ArticleID=21758&Key=Windows%202000%20Professional Article discussing advancements to Windows XP and how they benefit installation tasks.
http://www.wired.com/news/print/0,1294,42907,00.html News story from wired.com regarding release of Windows XP.
http://support.microsoft.com/support/kb/articles/Q234/9/26.ASP Microsoft support article about the sample security templates that ship with Windows 2000.
http://www.sans.org/infosecFAQ/win2000/standalone.htm SANS article that describes steps to harden or ”lock down” a stand-alone Windows 2000 Professional system.
http://www.labmice.net/articles/securingwin2000.htm LabMice checklist/article for steps to secure an installation of Windows 2000 professional.
http://support.microsoft.com/support/kb/articles/Q249/1/49.ASP Microsoft Tip for installing Windows 2000 along with Windows hotfixes in one step.

Hyperlink URL and Description
http://help.netscape.com/communicator/install_guide.html Installation guide for Netscape 4.78 and later versions on Windows 2000.
http://www.winntmag.com/Articles/Index.cfm?ArticleID=7619 Winntmag.com is a part of windows2000mag.com. This is a list of some installation tips for Windows 2000.
http://www.vmware.com/support/reference/common/guest_win2000.html Article describing known problems with installing Windows 2000 versions with VMWare.
http://www.winntmag.com/Articles/Index.cfm?ArticleID=7700 A post-installation checklist for Windows 2000.
http://www.itp-journals.com/search/e1218.htm Article describing automated Windows 2000 professional installations
http://www.arstechnica.com/paedia/n/ntfs/ntfs5-1.html Two-part article discussing changes in NTFS 5.0 within Windows 2000 including advancements to ACL.
http://www.sans.org/infosecFAQ/e-mail/sec_outlook.htm A SANS article on possible steps to take to secure Microsoft Outlook.
http://www.europe.f-secure.com/virus-info/u-vbs/remove-vbs-w2k.shtml Resource detailing how to remove the VBS extensions from the known list. This safeguards against VBS worms and viruses.
http://www.eudora.com A Web site for the Eudora e-mail program.
http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci214077,00.html The whatis.com page for the LDCM from Intel.
http://www.Webopedia.com/TERM/L/LDCM.html More on LDCM.

Hyperlink URL and Description
http://www.aelita.com/library/whitepapers/SnapReports/SMSinvestment.pdf White paper on SMS.
http://www.exchangeadmin.com/Articles/Index.cfm?ArticleID=4837&Key=Outlook%20Personal%20Folders Article describing personal file folders and their security for stand-alone users of Microsoft Outlook.
http://home.cnet.com/software/0-3923245-7-1498886.html Cnet.com article on the Windows 2000 Professional OS.

Appendix F—Other References

Table F-1 is a comprehensive list of Internet links providing dedicated resources for reference on Windows 2000 Professional security best practices. This list is meant as a supplemental resource to the System Administration Guidance for Securing Microsoft Windows 2000 Professional Systems document.

Although thousands of Internet sites provide valuable security information about the Windows 2000 operating system and other Microsoft products, this list is focuses on those Internet sites that strive to provide security-centered reference services.

Table F-1. Computer Security Links

Hyperlink URL and Description
http://is-it-true.org/nt/nt2000/ Personal resource site for Windows 2000 administrators.
http://microsoft.com/windows/ie/evaluation/overview/privacy.asp Internet Explorer 6 Web privacy technology overview. IE 6 now includes support for the P3P standard.
http://msdn.microsoft.com Development reference site for all of Microsoft's product line. Includes valuable reference for developers of Windows 2000 Professional software.
http://Web.mit.edu/kerberos/www/ MIT reference page for Kerberos. This link is meant as a reference page because it does not provide direct information regarding the role of Kerberos within the Windows 2000 architecture.
http://windows2000.about.com/cs/security/ Subsection of about.com for topics and articles written that pertain directly to Windows 2000 security issues. This site is maintained by Douglas Ludens.
http://windowsupdate.microsoft.com Personalized ActiveX (critical components installer) driven Web site providing latest updates and previews of Microsoft software. This site is extremely valuable for the end-user.
http://www.activewin.com/win2000/index.shtml A Microsoft-sponsored site containing vulnerability information and associated patch information.

Hyperlink URL and Description
http://www.cert.org Computer Emergency Response Team. The most famous incident response center. Provides highly detailed reports (Advisories) of newly reported vulnerabilities, including those affecting Windows 2000 and related Microsoft products.
http://www.labmice.net A Windows 2000 resource index that contains links to internal and external documents written on a variety of topics relating to Windows 2000.
http://www.microsoft.com/technet/ Home of Microsoft reference site for non-development technologies of Microsoft product line. This site provides extremely valuable information on Windows 2000 Professional.
http://www.microsoft.com/windows2000 The Microsoft Windows 2000 home page. This site is a great starting block for information regarding Windows 2000 security.
http://www.microsoft.com/windows2000/technologies/security/default.asp Learn more about Windows 2000 Security Services, including security management using the Microsoft Security Configuration Tool Set, support for IP security, the encrypting file system, public key infrastructure, smart cards, and Kerberos. This Microsoft corporate site can be trusted to be well maintained. This site should be seen as an index page to specific technology links that are seen below.
http://www.sans.org/infosecFAQ/ SANS site for information security reference. This site contains many articles relating directly to Windows 2000.
http://www.securityfocus.com/ Microsoft-specific content contains articles with keystroke level fixes for securing Microsoft machines. Must navigate directly to Microsoft section from navigation bar at the top of the Security Focus index page. This site provides a Web-based interface to a highly granular vulnerability database.
http://www.win2000mag.com/ Online magazine site featuring articles on various topics concerning Windows 2000.

Hyperlink URL and Description
http://www.windowsitlibrary.com Informative reference site for Windows product line. Note: this site is part of the Windows 2000 magazine network. (www.win2000mag.com)
http://www.windowsitsecurity.com/ Online news site specializing in information security issues within the Windows operating system product lines. This site provides limited access to its content based on a subscription service.
http://www.wininformant.com Additional site part of Windows 2000 magazine network. Authored by Paul Thurrott.
http://xforce.iss.net Xforce, which is a service of Internet Security Services, is a comparable vulnerability database to Security Focus or CERT.
http://ntsecurity.nu A Windows NT and Windows 2000 security site featuring vulnerability alerts and valuable tools available for download. This site is run by Arne Vidstrom.
http://www.isaserver.org/ This is a Web site dedicated to resources for the Microsoft ISA server.
http://www.swynk.com/sms/ Resource site dedicated to Microsoft SMS 2.0.

Security Reference List

This list provides a comprehensive source of security reference material. Table F-2 presents the list of reference materials pertaining to Windows 2000 Professional security.

Table F-2. Security Reference Book List

Title Author	Publisher	ISBN
Microsoft Windows 2000 Security Technical Reference		
Internet Security Systems	MS Press	0-7356-0858-X
Microsoft Windows 2000 Professional Expert Companion		
Craig Stinson and Carl Siechert	MS Press	0-7356-0855-5

Title Author	Publisher	ISBN
Microsoft Windows 2000 Professional Resource Kit		
Microsoft Corporation	MS Press	1-57231-808-2
Running Microsoft Windows 2000 Professional		
Craig Stinson and Carl Siechert	MS Press	1-57231-838-4
MCSE Training Kit: Microsoft Windows 2000 Professional		
Microsoft Corporation	MS Press	1-57231-901-1
Small Business Solutions for Microsoft Windows 2000 Professional		
Don Gilbert	MS Press	0-7356-0856-3
Inside Microsoft Windows 2000, Third Edition		
David A. Solomon, Mark E. Russinovich	MS Press	0-7356-1021-5
Windows 2000 Security		
Roberta Bragg	New Riders	0-7357-0991-2
MCSE ExamGear (70-220): Windows 2000 Network Security Design		
New Riders	New Riders	0-7357-1013-9
MCSE Training Guide (70-220): Designing Security for a Windows 2000 Network		
Roberta Bragg	New Riders	0-7357-0984-X
Windows NT/2000 Network Security		
E. Eugene Schultz	New Riders	1-5787-0253-4
Windows 2000 Virtual Private Networking		
Thaddeus Fortenberry	New Riders	1-5787-0246-1
Managing the Windows 2000 Registry		
Paul Robichaux	O'Reilly	1-56592-943-8
Windows 2000 Performance Guide		
Mark Friedman & Odysseas Pentakalos	O'Reilly	1-56592-466-5
Windows 2000 Administration in a Nutshell		
Mitch Tulloch	O'Reilly	1-56592-713-3
Mastering Windows 2000 Registry		
Peter D. Hipson	Sybex	0-7821-2615-4
Windows 2000 Complete		
Sybex Inc.	Sybex	0-7821-2721-5
Hacking Exposed Windows 2000: Network Security Secrets & Solutions		
Joel Scambray, Stuart McClure	McGraw-Hill	0-0721-9262-3
Windows 2000 Pro: The Missing Manual		
Sharon Crawford	O'Reilly	0-5960-0010-3

Title Author	Publisher	ISBN
Special Edition Using Microsoft Windows 2000 Professional		
Robert Cowart, Brian Knittel	Que	0-7897-2125-2
Windows 2000 Security Little Black Book: The Hands-On Reference Guide for Establishing a Secure Windows 2000 Network		
Ian McLean	The Coriolis Group	1-5761-0387-0
Windows 2000 Registry Little Black Book, 2nd Ed.		
Nathan Wallace, Anthony Sequeira, Nathan Walace	The Coriolis Group	1-5761-0882-1
Windows 2000 Registry*		
O. Kokoreva	Charles River Media	1584500816
Admin911: Windows 2000 Registry		
Kathy Ivens	McGraw-Hill	0-0721-2946-8
Windows 2000 Security Handbook		
N/A	McGraw-Hill	0072124334

The following Table F-3 lists publishers that have been cited for their works on Windows 2000 Professional security.

Table F-3. Major Computer Reference Publishers

Publisher	Internet URL
MS Press	http://mspress.microsoft.com
New Riders	http://www.newriders.com
Sybex	http://www.sybex.com
O'Reilly	http://www.oreilly.com/
Que	http://www.quepublishing.com/
The Coriolis Group	http://www.coriolis.com/
McGraw Hill	http://www.mcgraw-hill.com/

This page intentionally left blank

Appendix G—Summary of Recommendations

This Appenix reviews policy and practice recommendations made throughout the document for securing the Microsoft Windows 2000 Professional System.

- Security Analysis and Configuration Recommendation Summary
  - Use the **Security Configuration Analysis** snap-in and the **Local Security Policy** tool to import, analyze, modify, configure, and export the security settings.
  - Use the **GPO** to automate the deployment of security settings to domain member systems.
  - Use the **secedit.exe** tool in a script file to apply security settings to the Windows 2000 systems.
  - Apply the NIST template to configure the Security Options.
- Security Auditing and Logging Recommendations Summary
  - Apply the NIST template to configure the auditing and event log policies. Refer to Appendix B for specific recommended values.
  - Audit critical and sensitive personal data files.
  - In low-risk environments, use the **Event Viewer** weekly to review the log files; in higher risk environments, review the log files daily.
- Installation Summary
  - Partition the hard drive using NTFS for system and data files.
  - Install OS with minimum required services.
  - Install **Internet Protocol (TCP/IP)** networking and **Client for Microsoft Networking** only.
  - Secure the **winnt\repair** directory. The NIST security template does this automatically.
  - Create the ERD when security configuration is complete.
  - Securely store the ERD on removable media.
  - Delete or restrict access to the backup ERD from the **winnt\repair** directory.
- General security recommendations
  - Subscribe to the Microsoft Security mailing list and others.
  - Periodically scan systems to determine patch status using Windows Update Web site or the **hfnetchk.exe** tool.
  - Use the Microsoft Security site as a portal to search and download security patches.
  - Test and apply patches when required.
  - Update or create a new ERD after the system has been patched.
- Windows 2000 Professional configuration recommendations

- Secure the System and Data Partitions and restrict access to critical system files and utilities. Refer to Appendix B for specific recommended settings.
- Replace Everyone Group with Authenticated Users.
- Enable EFS to encrypt sensitive data at the folder or directory level.
- Remove the OS2 and POSIX system files.
- Disable Memory Dump.
- Set Recycle Bin to Automatically Delete Files.
- Disable LMHosts Lookup.
- Disable NetBIOS over TCP/IP when appropriate and block the tcp/udp 135 to 139 and 445 ports at the perimeter firewall or border router.
- Use personal firewall software to protect the systems connected to untrusted networks.
- Enable TCP/IP Filtering when possible.
- Enable IPsec Filtering when possible.
- Disable Unnecessary Services. Refer to Appendix B for specific recommended settings.
- Apply the NIST Security Template.
- Perform a backup of system data after any system modifications.
- Perform backups of user data on a regular schedule and test recovering from the backup archives.

- Administrator and User recommendations
  - Use a logon account with User group permissions for day-to-day account usage.
  - Use the Administrator account only when modifying or managing the system.
  - Apply the NIST template to configure the user rights assignment, account password policy, and account lockout policy. Refer to Appendix B for specific recommended settings.
  - Formulate a plan for dealing with ActiveX controls that cannot be downloaded under the secure User context. See Microsoft bulletins Q240897, Q241163, and Q280579.
  - Never logon with administrative privileges unless you need to perform administrative tasks. Use the runas.exe command instead.
- Anti-Virus Scanner Recommendation Summary
  - Do not install competing AntiVirus software on the same machine.
  - Ensure that AntiVirus scanners are configured properly and updated weekly or as often as a new virus is discovered.
  - Periodically perform a full scan of your system.

- Enable Auto-Protection scanning of new software and documents introduced to your system (all file types).
- Enable E-mail and Internet scanning.

- E-mail Client Recommendation Summary
  - Frequently update e-mail clients.
  - Disable Visual Basic Scripting in Microsoft Outlook.
  - Turn off the Outlook preview pane.
  - Display extensions for attachments.
  - Set Outlook's attachment security to HIGH.
  - Set Outlook's Macro Security level to HIGH.
  - Secure the users e-mail data directory.
  - Disable executables in HTML content in Eudora.
  - Deselect the Use Microsoft's viewer option in Eudora.
  - Enable message warnings in Eudora.
- Web Browser Recommendation Summary
  - Frequently update Web browsers.
  - Upgrade encryption level to 128 bits.
  - Disable Active Scripting if your organization requires a high level of security. **Note:** Disabling ActiveX will prevent Microsoft's automatic update sites from working properly.
- Office 2000 Productivity Application Recommendation Summary
  - Frequently update Office applications.
  - Set macro security level to HIGH.
  - Digitally Sign safe macros used within your environment.
  - Enforce installed Add-ins with the same security requirements as opening documents.
  - Protect temporary files created by Office 2000 applications.

This page intentionally left blank

Appendix H—Acronyms

ACL	Access Control List
AOL	America On-line
API	Applications Programming Interface
AS	Authentication Server
ATM	Asynchronous Transfer Mode
CD	Compact Disk
CERT	Computer Emergency Response Team
CIS	The Center for Internet Security
COTS	Commercial off the Shelf Product
CRL	Certificate Revocation List
CS	Client/Server
DAC	Discretionary Access Control
DACL	Discretionary Access Control List
DES	Data Encryption Standard
DESX	Expanded Data Encryption Standard
DHCP	Dynamics Host Configuration Protocol
DISA	Defense Information Systems Agency
DLL	Dynamic Link Library
DNS	Domain Name System
DoD	Department of Defense
EFS	Encrypted File System
e-mail	Electronic mail
ERD	Emergency Repair Disk
FAT	File Allocation Table
FEK	File Encryption Key
FTP	File Transfer Protocol
GB	GigaByte
GINA	Graphical Identification and Authentication
GPO	Group Policy Object
GUI	Graphical User Interface
HKCQ	Hkey_Current_Config
HKCR	HKey_Classes_Root
HKCU	HKey_Current_User
HKLM	HKey_Local _Machine
HKU	Hkey_Users
HTML	Hypertext Markup Language
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IE	Internet Explorer
IEAK	Internet Explorer Administrators Kit
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IPsec	IP Security
IT	Information Technology
ITL	Information Technology Laboratory
JVM	Java Virtual Machine
L2TP	Layer Two Transport Protocol
LAN	Local Area Network

LM	Lan Manager
MFT	Master File Table
MMC	Microsoft Management Console
NAI	Network Associates
NetBT	NetBios over TCP/IP
NIST	National Institute of Standards
NSA	National Security Agency
NTFS	New Technology File System
NTLM	Windows NT LanManager
OESU	Outlook E-mail Security Update
OMB	Office of Management and Budget
OS	Operating System
OU	Organizational Units
PC/SC	Personal Computer/Smart Card
PIN	Personnel Identification Number
PKI	Public Key Infrastructure
POSIX	Portable Operating System Interface for Computer Environments
PPTP	Point-to-Point Tunneling Protocol
PXE	Pre-boot eXecution Environment
RCE	Route Cache Entry
RFC	Request for Comment
RIS	Remote Installation Service
RPC	Remote Procedure Call
RSVP	Resource Reservation Protocol
SA	System Administrator
SACL	System Access Control List
SAM	Security Accounts Manager
SANS	SysAdmin, Audit, Network, Security Institute
SFC	System File Checker
SID	Security Identify
SMB	Server Message Block
SMS	Systems Management Server
SMTP	Simple Mail Transport Protocol
SP3	Microsoft Service Pack
SQL	Structured Query Language
SR	Service Release
SSL	Secure Socket Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
TGS	Ticket Granting Ticket
TGT	Ticket-Granting Ticket
UPS	Uninterruptible Power Supply
URL	Uniform Resource Locator
VBA	Visual Basic for Application
VBS	Visual Basic Script
WFP	Windows File Protection
Win2k Pro	Windows 2000 Professional System
WMI	Windows Management Instrumentation
WSH	Windows Scripting Host

Appendix I—Index

A

Access Control List, iv, vi, 6-1, 8-1, 8-2, 8-3, 8-4, 9-2, 9-4, 10-28, A-2, D-3, E-7, H-3
America On-line, 10-26, H-4
Applications Programming Interface, 8-9, A-1, H-3
Asynchronous Transfer Mode, 2-3, H-2
Authentication Server, 2-1, H-2

C

Certificate Revocation List, 2-1, 2-2, H-2
Client/Server, 2-1, H-2
Commercial off the Shelf Product, 3, 10-1, H-1
Compact Disk, 4-9, 6-2, 7-1, 10-2, 10-30, 11-2, A-2, A-6, A-7, B-9, H-4
Computer Emergency Response Team, 7-4, 10-22, F-3, H-4

D

Data Encryption Standard, 2-3, D-3, H-2
Defense Information Systems Agency, 1, H-1
Department of Defense, B-11, H-5
Discretionary Access Control, 6-1, H-3
Discretionary Access Control List, 9-2, H-4
Domain Name System, H-3
Dynamic Link Library, 9-4, 10-29, A-8, H-4
Dynamics Host Configuration Protocol, 8-13, 8-18, 11-1, B-13, H-3

E

Electronic mail, 3, 4, 1-3, 8-16, 10-1, 10-2, 10-3, 10-4, 10-5, 10-7, 10-8, 10-9, 10-12, 10-16, 10-33, 10-34, E-7, G-3, H-1
Emergency Repair Disk, iii, vi, 2, 3, 6-3, 6-4, 6-5, 6-6, 7-1, 7-5, 8-20, E-2, G-1, G-2, H-1
Encrypted File System, iv, vi, 2-1, 2-3, 8-1, 8-4, 8-5, 8-7, 8-8, 8-20, D-3, D-4, D-5, E-1, E-2, G-2, H-2
Excel, 10-32, 10-33
Expanded Data Encryption Standard, 2-3, D-3, H-2

F

File Allocation Table, 6-1, H-3
File Encryption Key, 8-5, 8-7, H-3
File Transfer Protocol, 8-16, 10-25, B-13, H-3

G

GigaByte, B-11, H-5
Graphical Identification and Authentication, 2-2, H-2
Graphical User Interface, 2, 10-1, H-1
Group Policy Object, 4-6, 4-7, 4-10, G-1, H-2

H

HKey_Classes_Root, 10-26, A-1, H-4
Hkey_Current_Config, H-4
HKey_Current_Usre, A-1, H-4
HKey_Local _Machine, 8-14, 10-26, A-1, A-3, A-4, H-4
Hkey_Users, A-1, H-4
Hypertext Markup Language, vii, 4, 10-19, 10-20, 10-34, G-3, H-1

I

Information Technology, 1-1, H-1
Information Technology Laboratory, iii, H-1
Internet Control Message Protocol, A-9, H-5
Internet Engineering Task Force, 2-1, 2-2, H-2
Internet Explorer, 1, 7-3, 10-10, 10-21, 10-22, 10-24, 10-25, 10-29, E-2, E-3, F-1, H-1
Internet Explorer Administrators Kit, 10-25, H-4
Internet Key Exchange, 8-14, H-3
Intrusion Detection System, 8-12, H-3
IP Security, iii, iv, 2-1, 2-2, 2-3, 8-7, 8-14, 8-15, 8-16, 8-17, 8-21, B-13, G-2, H-2

J

Java Virtual Machine, vii, 10-23, 10-24, H-4

L

Lan Manager, 2-1, 4-8, B-7, B-13, H-2
Layer Two Transport Protocol, iii, 2-1, 2-3, H-2
Local Area Network, 4-8, 8-12, B-7, H-3

M

Macro, iv, vii, 4, 10-15, 10-16, 10-32, 10-34, G-3
Master File Table, 6-1, H-3
Microsoft Management Console, vi, 4-1, 4-2, 4-7, 5-1, 8-1, 8-17, 8-20, 9-5, B-2, C-1, D-8, H-2
Microsoft Service Pack, 7-1, H-3

N

National Institute of Standards, iii, 1, v, vii, 1, 2, 3, 1-1, 1-2, 1-3, 4-1, 4-2, 4-4, 4-10, 5-1, 5-4, 6-1, 6-2, 6-6, 7-1, 8-1, 8-12, 8-14, 8-18, 8-20, 8-21, 9-1, 9-7, 9-8, 10-1, 10-32, 11-1, A-5, B-1, B-3, B-12, B-24, B-28, G-1, G-2, H-1
National Security Agency, 1, 1-1, 4-1, 10-33, B-2, B-11, E-1, H-1
NetBios over TCP/IP, 8-13, H-3
Network Associates, 1, 10-2, H-4
New Technology File System, iii, vi, 2, 2-3, 4-8, 5-1, 5-3, 6-1, 6-2, 6-5, 6-6, 7-3, 8-1, 8-2, 8-4, 8-7, 8-18, 9-3, 9-4, B-6, D-3, E-7, G-1, H-1

O

Office, iii, 1, iv, vii, 4, 5, 1-1, 1-3, 10-2, 10-9, 10-10, 10-15, 10-30, 10-31, 10-32, 10-33, 10-34, E-3, E-4, G-3, G-4, H-1
Office of Management and Budget, 1-1, H-1
Operating System, 2, 3, 2-1, 2-2, 3-1, 4-1, 6-1, 6-4, 6-6, 7-1, 7-3, 8-8, 8-9, 8-11, 8-20, 9-2, 9-5, 10-10, 10-21, 11-1, 11-2, A-1, A-6, A-8, B-24, D-1, D-3, E-8, G-1, H-1
Organizational Units, 3-1, 4-5, 4-6, 8-20, 11-1, H-2
Outlook E-mail Security Update, 4, H-1

P

Personal Computer/Smart Card, 2-1, H-2
Personnel Identification Number, 2-2, H-2
Point-to-Point Tunneling Protocol, iii, 2-1, 2-3, H-2
Portable Operating System Interface for Computer Environments, iv, 8-8, 8-9, 8-10, 8-20, G-2, H-3
Pre-boot eXecution Environment, 11-1, H-4
Public Key Infrastructure, iii, 2-1, 2-2, 8-5, H-2

R

Remote Installation Service, 11-1, H-4
Remote Procedure Call, 7-2, 8-19, B-14, H-3
Request for Comment, 2-1, A-10, H-2
Resource Reservation Protocol, 8-14, 8-15, B-14, H-3
Route Cache Entry, A-10, H-5

S

Secure Socket Layer, 7-2, 8-7, H-3
Security Accounts Manager, vi, 3-1, 6-4, 6-5, A-4, H-2
Security Identify, 8-2, 9-2, H-3
Server Message Block, 4-9, 8-16, A-8, B-10, H-3
Service Release, 10-31, H-4
Simple Mail Transport Protocol, 7-2, B-14, H-5
Structured Query Language, 7-2, A-7, B-13, B-14, H-4
SysAdmin, Audit, Network, Security Institute, 1, 4-1, 10-22, E-4, E-6, E-7, F-2, H-1
System Access Control List, 5-2, B-3, B-6, H-5
System Administrator, 1, 1-1, 8-18, 9-1, 10-28, 11-2, 11-1, A-9, B-3, D-8, H-1
System File Checker, A-5, H-4
Systems Management Server, 1, 1-3, 11-1, 11-2, E-8, F-3, H-1, H-4

T

Template, vi, vii, 4-3, 4-5, 8-1, 8-19, 8-21, 9-8, B-1, B-3, G-2
The Center for Internet Security, 1, H-1
Ticket Granting Ticket, 2-1, H-2
Ticket-Granting Ticket, 2-2, H-2
Transmission Control Protocol/Internet Protocol, iv, 2, 2-3, 6-1, 6-6, 8-12, 8-13, 8-14, 8-15, 8-21, A-9, B-14, G-1, G-2, H-1, H-3

U

Uniform Resource Locator, 7-1, 7-4, 10-25, 10-26, 10-30, D-1, E-1, F-1, F-5, H-3
Uninterruptible Power Supply, 8-19, H-3

V

Visual Basic for Application, 10-30, 10-32, 10-33, H-4
Visual Basic Script, 10-10, 10-12, 10-33, E-7, H-4

W

Windows 2000 Professional System, H-1
Windows File Protection, A-5, H-4
Windows Management Instrumentation, 8-19, A-4, B-26, H-3
Windows NT LanManager, 2-1, 4-8, H-2
Windows Scripting Host, 10-10, E-2, H-4