



**National Institute of
Standards and Technology**

Technology Administration
U.S. Department of Commerce

Special Publication 800-43

System 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*

Version 2002.01.28

Send Comments to itsec@nist.gov

NIST Special Publication 800-43

System 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*

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

January 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

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, 163 pages (Dec. 2001)

<p>Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.</p>

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

Disclaimer

Certain products are described in this document as examples only. Inclusion or exclusion of any product does not imply endorsement or non-endorsement by NIST or any agency of the U.S. Government. Inclusion of a product name does not imply that the product is the best or only product suitable for the specified purpose.

Acknowledgements

The authors Murugiah Souppaya of NIST and Anthony Harris, Nikolaos Selimis, and Mark McLarnon of Booz Allen and Hamilton wish to thank Timothy Grance and John Wack, staff at NIST, the National Security Agency, Microsoft, and the Security Professional community for providing valuable contributions to the technical content of this guide.

Trademark Information

Microsoft, MS-DOS, Windows, Windows 2000, Windows NT, SMS, Systems Management Server, Internet Explorer, IE, Microsoft Office, Outlook, and Microsoft Word are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and other countries.

Symantec and Norton AntiVirus are registered trademarks of Symantec Corporation.

Netscape and Netscape Communicator are registered trademarks of Netscape Communications Corporation.

McAfee, VirusScan, Network Associates, and NAI are registered trademarks of Network Associates Technology Incorporated.

F-Secure is a registered trademark of F-Secure Incorporated.

Qualcomm and Eudora are registered trademarks of Qualcomm Incorporated.

IBM and LanDesk are registered trademarks of IBM Corporation.

All other names are registered trademarks or trademarks of their respective companies.

Table of Contents

1. INTRODUCTION.....	1
1.1 AUTHORITY	1
1.2 PURPOSE AND SCOPE.....	2
1.3 OBJECTIVE	2
1.4 AUDIENCE AND ASSUMPTIONS	2
1.5 DOCUMENT STRUCTURE	2
2. WINDOWS 2000 SECURITY COMPONENTS OVERVIEW	4
2.1 KERBEROS SUPPORT	4
2.2 SMART CARD LOGON SUPPORT	5
2.3 PKI SUPPORT.....	5
2.4 IPSEC SUPPORT	5
2.5 PPTP AND L2TP SUPPORT.....	6
2.6 ENCRYPTING FILE SYSTEM SUPPORT	6
3. STANDALONE VS DOMAIN MEMBER	7
3.1 STANDALONE.....	7
3.2 DOMAIN	7
4. SECURITY CONFIGURATION TOOL SET	9
4.1 WINDOWS 2000 SECURITY TEMPLATES.....	9
4.2 ANALYSIS AND CONFIGURATION	10
4.3 GROUP POLICY DISTRIBUTION	13
4.4 SECEDIT	14
4.4.1 Secedit Syntax.....	14
4.4.2 Secedit Advantages	15
4.5 CREATING SECURITY TEMPLATES.....	15
4.6 SUMMARY OF RECOMMENDATIONS	18
5. AUDITING AND EVENT LOGGING	19
5.1 SYSTEM-WIDE AUDITING	19
5.2 INDIVIDUAL FILE AUDITING.....	21
5.3 SUMMARY OF RECOMMENDATIONS	22
6. WINDOWS 2000 PROFESSIONAL INSTALLATION	23
6.1 WHY CHOOSE NTFS?.....	23
6.2 HOW TO CONVERT NON-NTFS PARTITIONS	24
6.3 OTHER SETTINGS.....	24
6.4 CREATING AND PROTECTING THE ERD	24
6.4.1 How to Create an ERD.....	25
6.4.2 How to Protect ERD	26
6.4.3 How to Protect ERD Backup	26
6.5 SUMMARY OF RECOMMENDATIONS	27
7. UPDATING AND PATCHING GUIDELINES	28
7.1 WINDOWS 2000 PROFESSIONAL UPDATES	28
7.2 WINDOWS 2000 PATCHING RESOURCES	29

7.2.1	<i>Internet Security Portals</i>	29
7.2.2	<i>Windows Update Web Site</i>	30
7.3	SUMMARY OF RECOMMENDATIONS	31
8.	WINDOWS 2000 PRO CONFIGURATION GUIDELINES	32
8.1	SECURING THE FILE SYSTEM USING ACLS	32
8.1.1	<i>File System ACL</i>	32
8.1.2	<i>Setting ACLs</i>	32
8.1.3	<i>ACL Example</i>	33
8.1.4	<i>Windows 2000 Access Control</i>	33
8.1.5	<i>Replace Default Access Rights</i>	35
8.2	ENCRYPTED FILE SYSTEM.....	35
8.2.1	<i>How Does EFS Work?</i>	35
8.2.2	<i>How Is EFS Implemented?</i>	35
8.2.3	<i>EFS Example</i>	36
8.2.4	<i>EFS Data Recovery</i>	38
8.3	ADDITIONAL FILE SYSTEM SECURITY MEASURES	39
8.3.1	<i>Removal of OS2 and POSIX</i>	39
8.3.2	<i>Prevent Data Remnants</i>	40
8.4	SECURING THE NETWORK INTERFACE.....	42
8.4.1	<i>TCP/IP Port Filtering</i>	44
8.4.2	<i>IPSEC Filtering</i>	44
8.5	DISABLING UNNECESSARY SERVICES	47
8.5.1	<i>Applying the Security Template</i>	51
8.6	DOMAIN MEMBER MACHINE CONFIGURATION	51
8.7	SUMMARY OF RECOMMENDATIONS	52
9.	ADMINISTRATOR, POWER USERS AND USERS	53
9.1	WINDOWS 2000 SECURITY IDENTIFIER	53
9.2	ADMINISTRATOR ACCOUNT	53
9.3	POWER USERS GROUP.....	54
9.4	USERS GROUP	56
9.5	CHANGE ACCOUNT GROUP MEMBERSHIP	58
9.6	ACCOUNT POLICIES	60
9.7	SUMMARY OF RECOMMENDATIONS	61
10.	APPLICATION SPECIFIC CONFIGURATION.....	62
10.1	ANTI-VIRUS SCANNERS	62
10.1.1	<i>McAfee Virus Scan</i>	63
10.1.2	<i>Norton AntiVirus</i>	66
10.1.3	<i>F-Secure Antivirus</i>	68
10.2	EMAIL CLIENTS.....	70
10.2.1	<i>Microsoft Outlook Security</i>	70
10.2.2	<i>Qualcomm Eudora</i>	76
10.3	WEB BROWSERS	80
10.3.1	<i>Internet Explorer</i>	80
10.3.2	<i>Netscape Navigator</i>	84
10.4	PRODUCTIVITY APPLICATIONS.....	89
10.4.1	<i>Microsoft Office Installation Issues</i>	89
10.4.2	<i>Microsoft Office Updates</i>	90
10.4.3	<i>Office 2000 Macro Virus Security</i>	90
10.5	SUMMARY OF RECOMMENDATIONS	92
11.	REMOTE SYSTEM SEAT MANAGEMENT.....	94

11.1	SOFTWARE INSTALLATION	94
11.2	CHANGE AND CONFIGURATION MANAGEMENT	95
11.3	ADD ON MANAGEMENT SOFTWARE	95
12.	SUMMARY	97
APPENDIX A: REGISTRY DISCUSSION		98
APPENDIX B: NIST WINDOWS 2000 SECURITY TEMPLATES.....		114
APPENDIX C: TOOLS.....		130
APPENDIX D: WINDOWS XP SECURITY COMPONENTS OVERVIEW.....		132
APPENDIX E: REFERENCES USED IN THIS DOCUMENT		139
APPENDIX F: OTHER REFERENCES.....		147

List of Figures

Figure 4-1: MMC Console.....	10
Figure 4-2: Create New Database	11
Figure 4-3: Select Template.....	11
Figure 4-4: Analysis of Current Settings	12
Figure 4-5: Change database settings	12
Figure 4-6: Configure Computer Settings.....	13
Figure 4-7: Windows 2000 Local Security Settings Node	16
Figure 4-8: Windows 2000 Local Security Policy Export.....	18
Figure 5-1: Event Viewer.....	19
Figure 5-2: System-Wide Audit Policy.....	20
Figure 5-3: Advanced File Settings	21
Figure 5-4: File Auditing	22
Figure 6-1 Open Windows 2000 Backup and Recovery Tools	25
Figure 6-2 Backup ERD showing SAM file	26
Figure 6-3 Restrict NTFS permissions for winnt\repair directory.....	27
Figure 7-1: Windows Update Web Site	30
Figure 8-1: ACL for sample system partition	33
Figure 8-2: Advanced ACL window for sample system partition.....	34
Figure 8-3: Advanced ACL window for sample system partition.....	34
Figure 8-4: Confirm application of EFS encryption to current resource	36
Figure 8-5: Directory listing with Sample Folder.....	36
Figure 8-6: Advanced Attributes window for Sample Folder	37
Figure 8-7: Updated folder listing of Sample Folder.....	37
Figure 8-8: Recovery Agent Default Setting	38
Figure 8-9: Updated folder listing of Sample Folder.....	40
Figure 8-10: Disable operating system memory dumps	41
Figure 8-11: Set Recycle Bin to Auto-Delete all Files	42
Figure 8-12: Disable LMHOSTS lookup and NetBIOS tunneling.....	43
Figure 8-13: Enable TCP/IP Port Filtering	44
Figure 8-14: A Sample IPSec Policy	47
Figure 8-15: Disable unnecessary Services screen	48
Figure 9-1: User Rights Assignment.....	58
Figure 9-2 Open Local Users and Groups from Computer Management.....	59
Figure 9-3: Account Properties box for example account client	60
Figure 9-4: Add user client to Backup Operators group.....	60
Figure 9-5: NIST template Password Policy	61
Figure 10-1: Update McAfee Virus Scan	64
Figure 10-2: McAfee Virus Scan update in progress.....	64
Figure 10-3: Configure McAfee e-mail scanning.....	65
Figure 10-4: Configure McAfee settings password protection.....	66
Figure 10-5: Set Norton Anti-virus Bloodhound detection levels	67
Figure 10-6: Set Norton Anti-virus automatic live update	68
Figure 10-7: F-Secure Anti-virus Real-time options window	69
Figure 10-8: F-Secure Anti-virus update options window	70
Figure 10-9: Windows 2000 Known File Types Window.....	72
Figure 10-10: Change behavior of Outlook after interacting with new message	73
Figure 10-11: Set Windows 2000 to display all known file extensions	74

Figure 10-12: Set Outlook Attachment Security to High	75
Figure 10-13: Set Outlook Security Zone	75
Figure 10-14: Set Outlook Macro Security.....	76
Figure 10-15: Eudora.ini properties file.....	77
Figure 10-16: Choose where to install Eudora data files.....	77
Figure 10-17: Eudora default directory permissions	78
Figure 10-18: Disable executables in HTML messages in Eudora.....	79
Figure 10-19: Enable executable warnings in Eudora	80
Figure 10-20: Disable Scripting in Internet Explorer	82
Figure 10-21: Disable Java in Internet Explorer.....	82
Figure 10-22: Set custom Microsoft JVM permissions	83
Figure 10-23: Confirm clearing cache on Internet Explorer.....	84
Figure 10-24: Registry Error Installing Netscape as a Regular User.....	85
Figure 10-25: Netscape Communicator Update Requesting Java Permission.....	86
Figure 10-26: Netscape Signed Java Applet/JavaScript Window	87
Figure 10-27: Disable Active Content within Netscape Communicator	88
Figure 10-28: Installed Netscape Plugins	89
Figure 10-29: Office 2000 Installation procedure	90

List of TABLES

Table 4-1: Secedit Syntax	14
Table 4-2: Local Security Policy List	16
Table 4-3: Settings for NIST2kws.inf Security Options.....	16
Table 5-1: System-wide audit policy description	20
Table 7-1: Articles Describing Bugs Fixed in Service Pack 2.....	29
Table 7-2: Information Security Portals	29
Table 8-1: Disable Unnecessary Windows 2000 Professional Services.....	48
Table 9-1 Default Access Control Settings for File System Objects.....	54
Table 9-2: Users' Write Access Locations	57
Table 9-3: Default User Rights	57
Table 10-1: Registry Keys Netscape Cannot Successfully Access During Installation	85

1. INTRODUCTION

Windows 2000 Professional has many valuable security features System Administrators 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 as well as recommended security settings for Windows 2000 Professional and selected applications.

System Administrators and users 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 Administrators in implementing security on their domain member and standalone Windows 2000 Professional workstations. The 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 upon 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 provides guidelines for Federal organizations' acquisition and use of security-related Information Technology (IT) products. These guidelines provide advice to agencies for sensitive (i.e., non-national security) unclassified systems. NIST's advice is given in the context of larger recommendations regarding computer systems security.

NIST developed this document in furtherance of its statutory responsibilities under the Computer Security Act of 1987¹ and the Information Technology Management Reform Act of 1996 (specifically section 15 of the United States Code (U.S.C.) 278 g-3(a)(5)). This 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 OMB Circular A-130, Appendix III.

The guidelines herein are not mandatory and binding standards. This document may be used voluntarily by non-governmental organizations. It is not subject to copyright.

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."*

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 Office of Management and Budget, or any other Federal official.

1.2 PURPOSE AND SCOPE

This document is intended to assist those responsible for the administration and security of Windows 2000 Professional systems by providing detailed information about security features of Windows 2000 Professional systems. This document is also intended to provide guidance to Administrators on securely configuring a Windows 2000 Professional workstation using security configuration templates and security checklists. Additional security configuration information is included for representative samples of key Windows applications. This document will benefit the advanced users who are interested in learning how to secure their Windows 2000 Professional system. The document is not intended to be used as a guideline to audit the configuration of Windows 2000 Professional system.

1.3 OBJECTIVE

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

1.4 AUDIENCE AND ASSUMPTIONS

The intended audience is Windows 2000 Systems Administrators, as well as technical Windows 2000 Professional users. This 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 twelve sections followed by six appendices. This subsection describes the structure of the document.

- Section 1 (this section) provides an introduction, authority, purpose and scope, objective, audience and assumption, and document structure.
- Section 2 of this document gives the reader a review of security components offered in the Windows 2000 Professional.
- Section 3 explains the differences between a Windows Standalone workstation and a Domain Member.
- Section 4 explains the use of the Security Configuration Tool Set.
- Section 5 presents Windows 2000 Professional security auditing.

NIST WIN2K DRAFT FOR PUBLIC COMMENT

- 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 the 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 Intel LanDesk and SMS can be used to enhance Windows 2000 Professional Security.
- Section 12, the summary, provides a brief review of the document.
- Appendix A provides an overview and 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.
- Appendix C lists some useful administration tools.
- Appendix D discusses some security components offered in Windows XP.
- Appendix E provides references used in this document.
- Appendix F lists other references to assist Administrators with further research and education.

2. WINDOWS 2000 SECURITY COMPONENTS OVERVIEW

The following section will present the various security components offered by the Windows 2000 Professional operating system. These new security features include: network authentication with Kerberos version 5, integrated 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 Protocol (IPSec) support is 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 within this section require configuration within the active directory of the Windows 2000 server and fall outside the scope of the 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) RFC 1510. The Kerberos protocol is composed of three subprotocols. The Authentication Service (AS) Exchange, Ticket-Granting Service (TGS) Exchange, and the Client/server (CS) Exchange. The Kerberos v.5 standard can only be used 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, if the Windows 2000 Domain Controller is configured to allow it. The older methods are still supported to allow legacy Windows clients to authenticate to a Windows 2000 domain environment. It should be noted that Kerberos could be only implemented by the Group Policy Object (GPO) in a Windows 2000 Domain, to be used for authentication to a Windows 2000 domain. Windows 2000 Professional standalone workstations and members of NT domains do not use Kerberos to perform local authentication, they will use the traditional NTLM. For Windows 2000 domain members Kerberos provides numerous benefits, including those below:

- **Efficiency.** Kerberos provides a client with credentials eliminating 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 have the ability to be two-way and transitive.
- **Interoperability.** The Windows 2000 Kerberos implementation is interoperable with other version 5 implementations of Kerberos clients.

2.2 SMART CARD LOGON SUPPORT

In the past, interactive logon meant the 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 version 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 only be used to log on 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 version 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 Microsoft integrated into Windows 2000 affects many core security functions of the operating system. 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 version 3 public key certificates and to provide compatibility with CRL version 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. For more information, refer to:

<http://www.microsoft.com/windows2000/en/advanced/iis/default.asp?url=/WINDOWS2000/en/advanced/iis/htm/core/iiabscsc.htm>

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. 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 IP Security 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 non-domain 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 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 IP Security, 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 ATM networks.

2.6 ENCRYPTING FILE SYSTEM SUPPORT

The 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 NTFS partition. EFS uses the Expanded Data Encryption Standard (DESX) algorithm, a variant of DES, by installing Service Pack 2 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.

3. STANDALONE VS DOMAIN MEMBER

This document focuses on two distinct configurations of Windows 2000 Professional workstation, Standalone and Domain Member. Each configuration has unique advantages and disadvantages.

3.1 STANDALONE

The Windows 2000 Professional Standalone 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, etc.) contained on the workstation is performed on the workstation using the local SAM (Security Accounts Manager). If users require remote access to the resources contained on the Windows 2000 Professional Standalone workstation they must authenticate directly to that machine. Every user that 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 their organization; the user must have a user id and password on each of the machines.

Each computer in a standalone (workgroup) configuration must be individually managed. Windows 2000 provides no built-in options for the centralized management of multiple workgroup computers. Therefore, each Windows 2000 Professional standalone 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. The base unit of the Windows 2000 domain model is the domain. 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 base 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. The Forest is a collection of non-contiguous 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 of the objects residing within the forest. Objects are entities such as a file, folder, printer, user, and computer system that are described by a distinct set of named attributes. The Active Directory uses Organizational Units (OU) to assist Administrators by allowing objects to be logically grouped together by function,

NIST WIN2K DRAFT FOR PUBLIC COMMENT

OS version, division, etc. to further simplify management, updates, and set Administrative boundaries.

OUs allow administrators 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 Administrators 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 was provided to give 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 Administrators with a centralized location to test and apply security policies for standalone and domain member Windows 2000 Professional systems. Use of the Security Configuration Tool Set and `secdit` command line interface is presented below. This document provides customized security templates for use with the Security Configuration Tool Set or `secdit`. These templates are described in Appendix B.

For more information about the Security Configuration Tool set please refer to:

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/deploy/confeat/securcon.asp>

4.1 WINDOWS 2000 SECURITY TEMPLATES

Windows 2000 Security Templates are used by the components of the Security Configuration Tool Set to provide standard security settings for comparison to existing security settings. The templates also provide input to the Security Configuration Tool Set to facilitate rapid application of standardized security settings across a Windows 2000 environment. The templates can be modified using the 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 level of security that will be achieved when the template is applied using `secdit` or the Security Configuration Manager MMC snap-in. The possible choices are: **basic**, **secure**, and **hsec** (which denotes high security). The **<operating system class level>** indicates what operating system the template is for. The possible choices include: **wk**, 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 **hsecws.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>

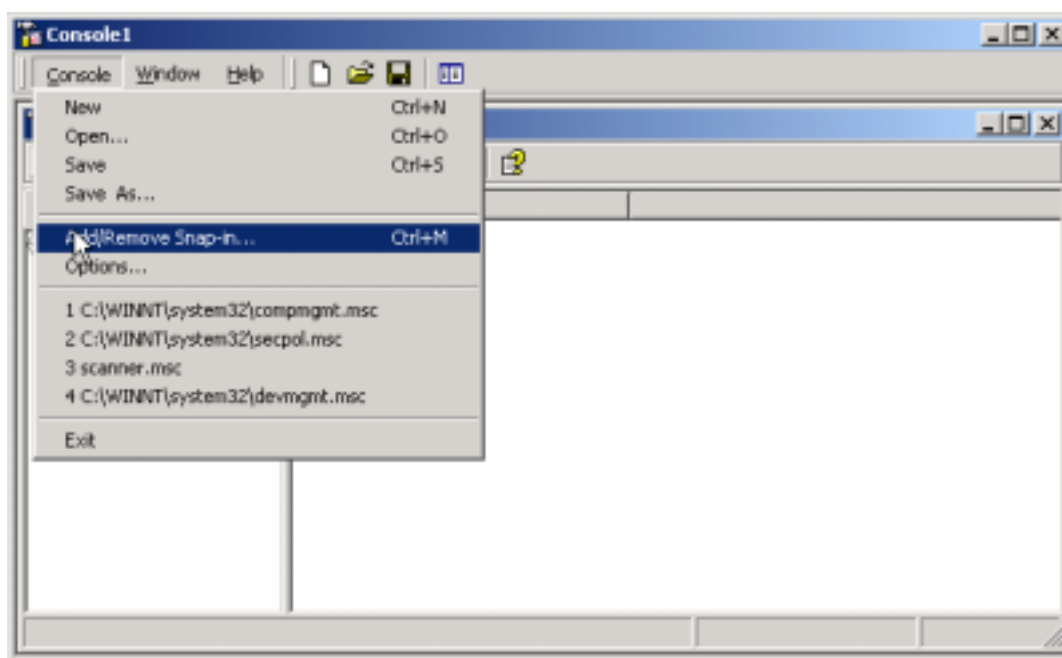
Appendix B contains NIST Win 2000 Professional security templates based on the National Security Agency (NSA) Windows 2000 security templates and recommendations. The included templates have been customized and fully documented for use on Windows 2000 Professional standalone and domain member workstations. The security template designed for a Windows 2000 Professional standalone workstation is named **NIST2kws.inf**. The template designed for a Windows 2000 Professional domain member is named **NIST2kdm.inf**.

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

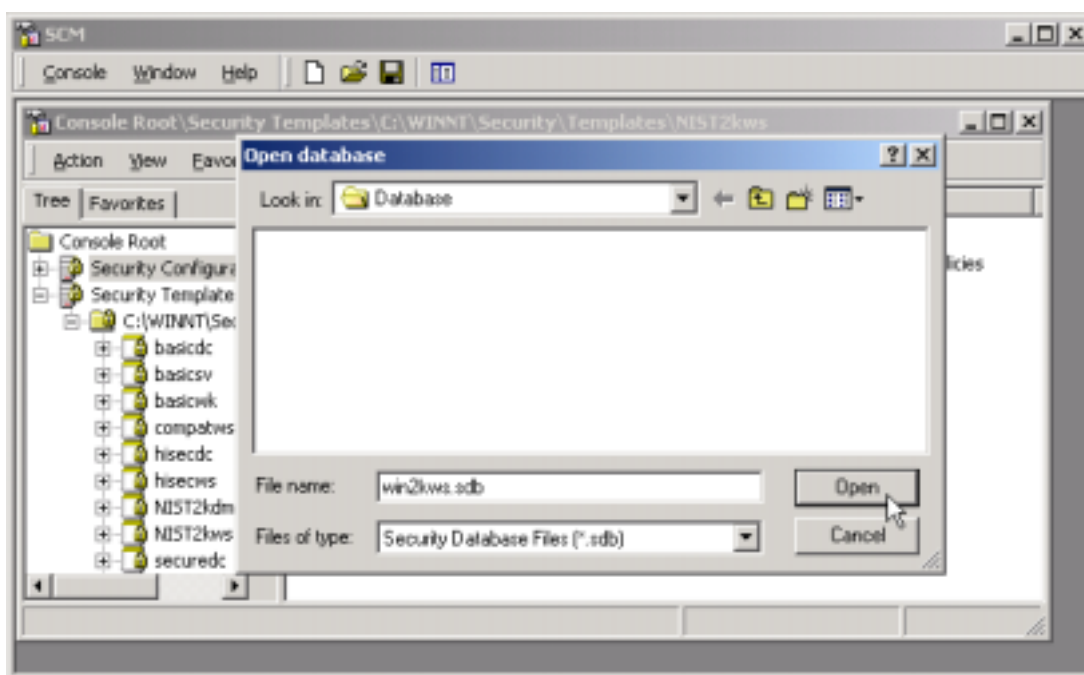
This section will discuss the analysis and configuration of a Windows 2000 Professional Workstation using the Security Configuration and Analysis Snap-in. The Snap-in can compare the current security settings of the workstation to pre-configured templates before they are applied. This allows Administrators the opportunity 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. Select **Console | Add/Remove Snap-in** menu, see Figure 4-1. When completed save the console in your **Administrative Tools** folder for future use.

Figure 4-1: MMC Console



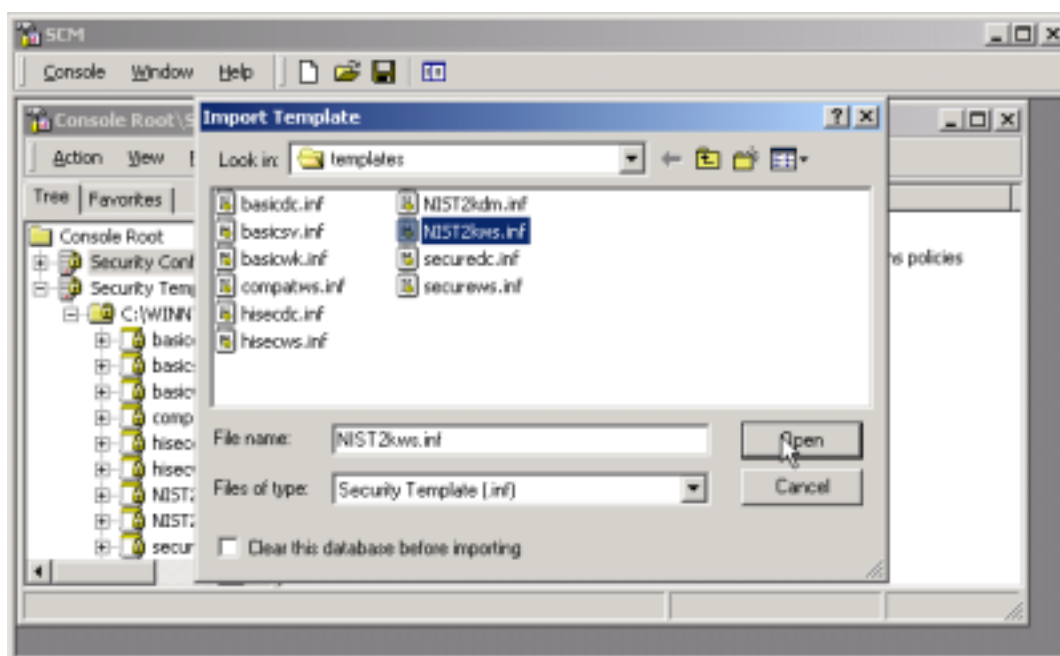
To use the NIST templates supplied with this document, copy them into the **%WINDIR%/Security/Templates** folder. Open a new database by right clicking **Security Configuration and Analysis** and selecting **open database**. Give the database a name and click open as shown in Figure 4-2.

Figure 4-2: Create New Database



Choose the template appropriate for your installation, **NIST2kws.inf** for standalone workstations and **NIST2kdm.inf** for domain member installations, and click **Open** to load the setting file as shown in Figure 4-3.

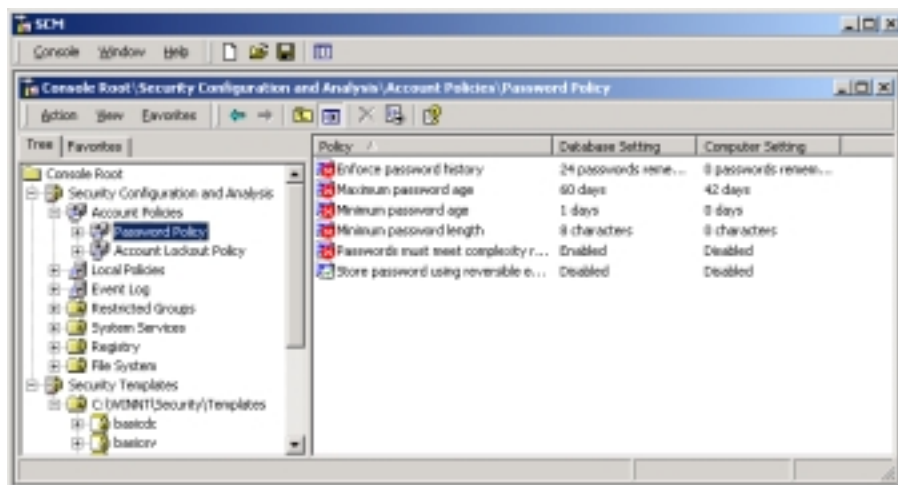
Figure 4-3: Select Template



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.

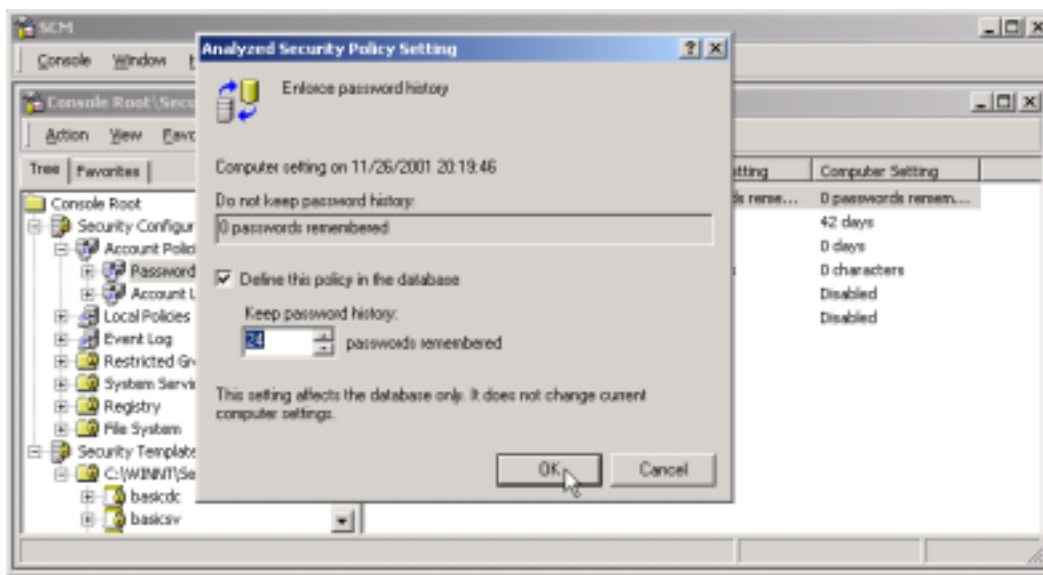
Seven categories of settings are listed under the Security Configuration and Analysis snap-in. Browse through these settings to view the differences between the templates and the computer configuration. Areas containing a red X differ from the template areas with a green check mark match the template and areas with neither a check 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: Analysis of Current Settings



If the reviewed settings need modification to match settings specific to the environment the computer resides in, 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.

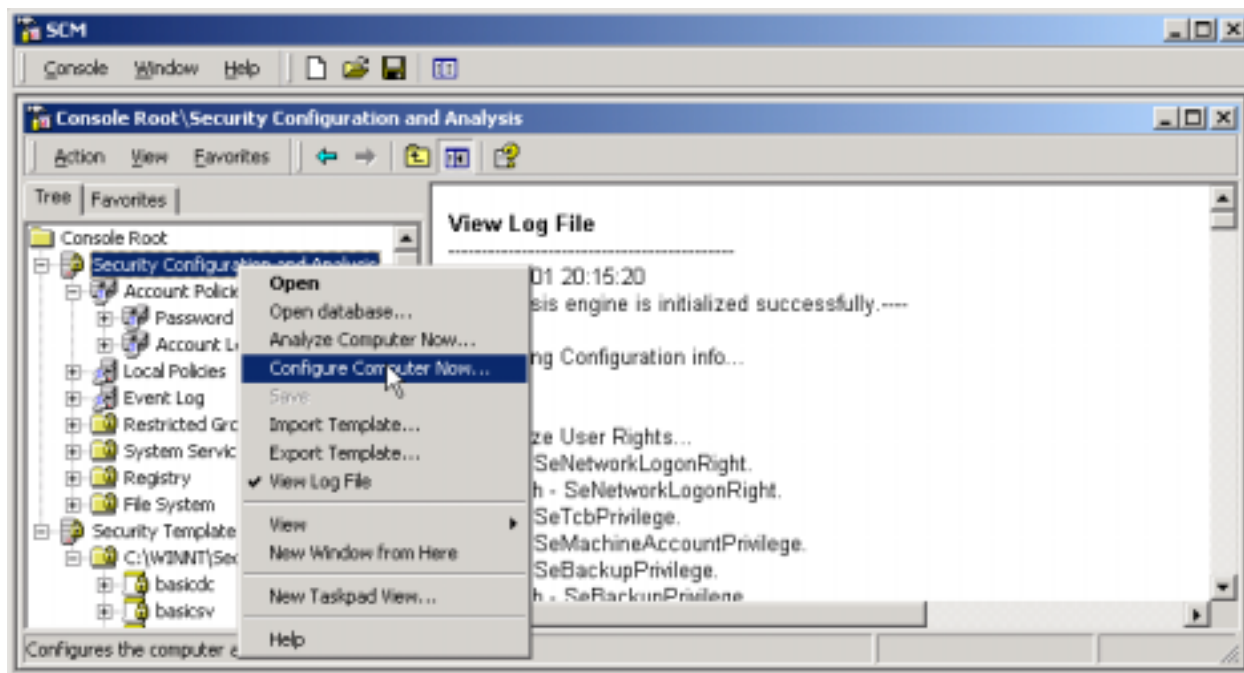
Figure 4-5: Change database settings



After all required changes 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 Organizational Unit (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.

1. Select the **Group Policy Object** linked to the OU containing the computers needing the security policy modification.
2. Expand **Computer Settings | Windows Settings**.
3. Right click **Security Settings** and choose **Import Policy**.
4. 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 only be applied using a Windows 2000 Server (Domain Controller) in a Windows 2000 domain environment (Active Directory). For more information about Active Directory and Group Policy, please 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 the 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 discusses possible switches that can be used with the **secedit** command.

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.
Options	<p>/MergedPolicy—merges and exports both domain and local policy settings.</p> <p>/DB filename—contains the filename and path to the database that contains the security template to be applied.</p> <p>/CFG filename—used with the /DB parameter. It specifies which security template will be imported into the database and applied to your system.</p> <p>/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.</p> <p>/areas area1 area2—Areas correspond with security policy</p>

Syntax	Description
	<p>categories: The categories are SECURITYPOLICY, GROUP_MGMT, USER_RIGHTS, REGKEYS, FILESTORE, and SERVICES.</p> <p>/Log logpath—contains the path to the log file created during the analysis.</p> <p>/verbose—gives you detailed progress information during the analysis.</p> <p>/quiet—suppresses the screen and log output.</p>

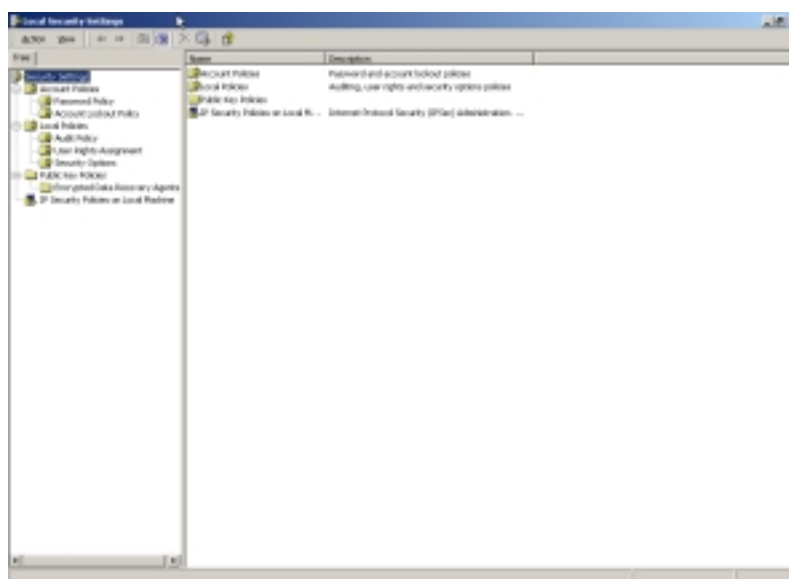
4.4.2 Secedit Advantages

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 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 Administrators 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 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 is discussed in Section 4.3.

4.5 CREATING SECURITY TEMPLATES

Windows 2000 Professional users have the capability 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 then distributed to computers within the enterprise, just as in the first method.

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

Figure 4-7: Windows 2000 Local Security Settings Node

The Local Security Settings node allows modification of the following 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 **NIST2kws.inf** template to provide an example of the various configuration choices provided by the Local Security Settings Policy Editor. Each of the Policies 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 NIST2kws.inf Security Options

Policy Description	Setting
Additional restrictions for anonymous connections	No access without explicit anonymous permissions
Allow server operators to schedule tasks (domain	Not defined

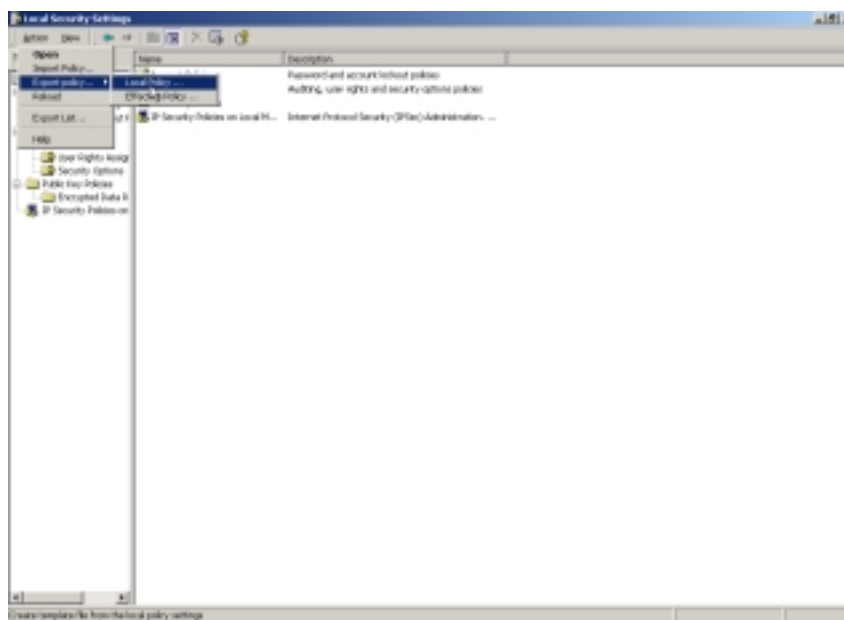
NIST WIN2K DRAFT FOR PUBLIC COMMENT

controllers only)	
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	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 not available)	0 logons
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 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 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	Enabled

(e.g. Symbolic Links)	
Unsigned driver installation behavior	Warn but allow installation
Unsigned non-driver 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



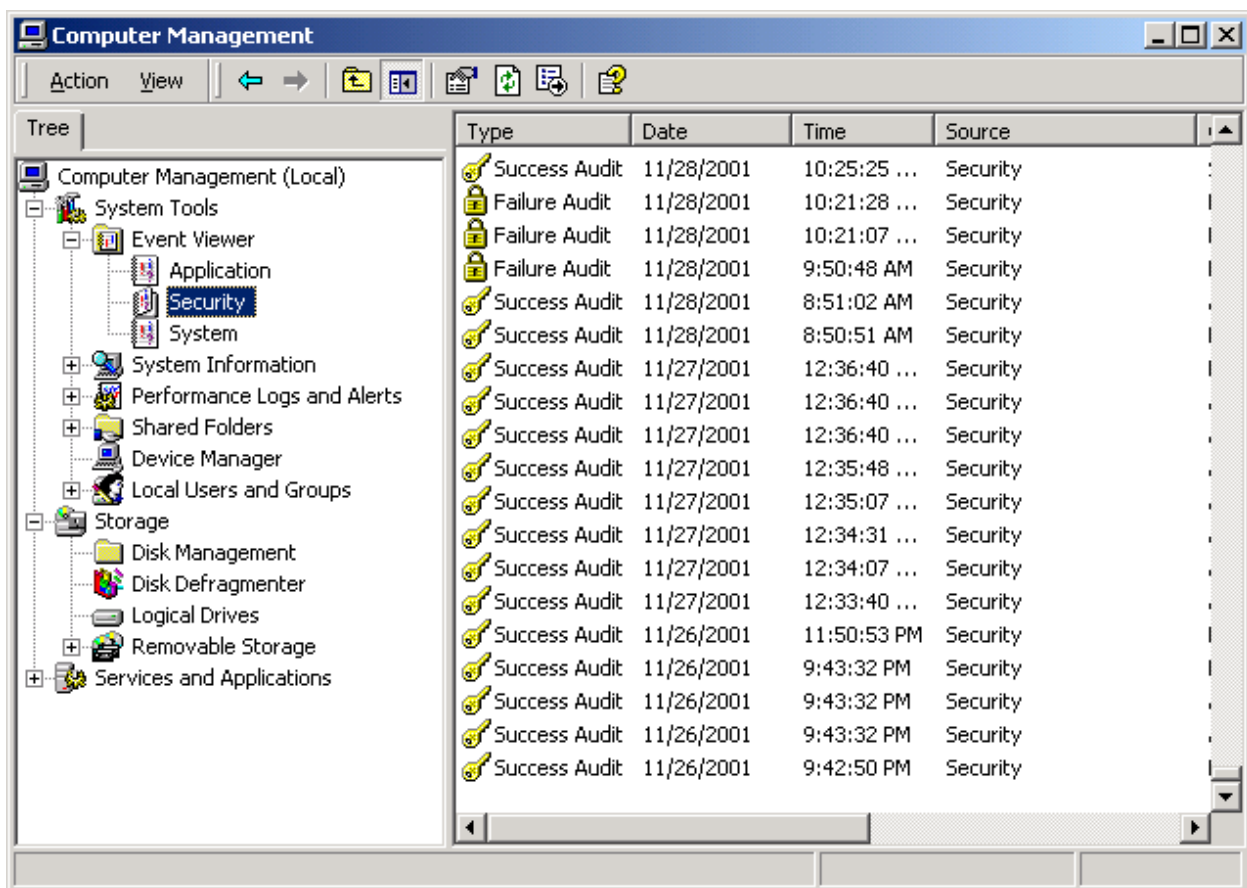
4.6 SUMMARY OF RECOMMENDATIONS

- 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

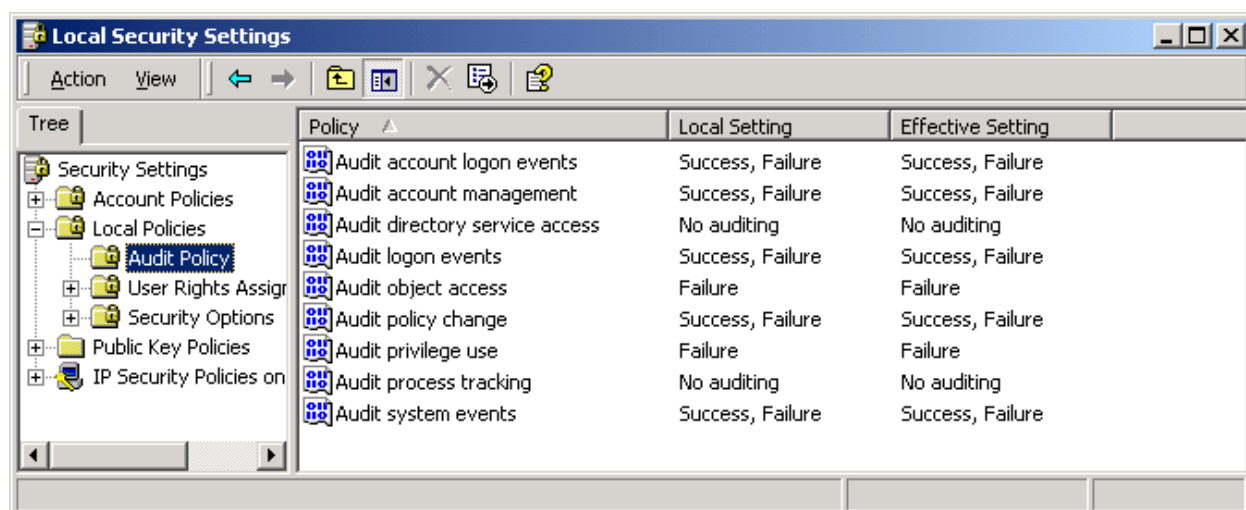
Windows 2000 Professional includes powerful auditing capabilities. Windows 2000 Professional performs system wide auditing of logon events, account management, directory service access, object access, policy change, privilege use, process tracking, and system events. Individual files in the NTFS file 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 SYSTEM-WIDE 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 as shown in Figure 5-2.

Figure 5-2: System-Wide Audit Policy

The policy areas are described in Table 5-1 below.

Table 5-1: System-wide audit policy description

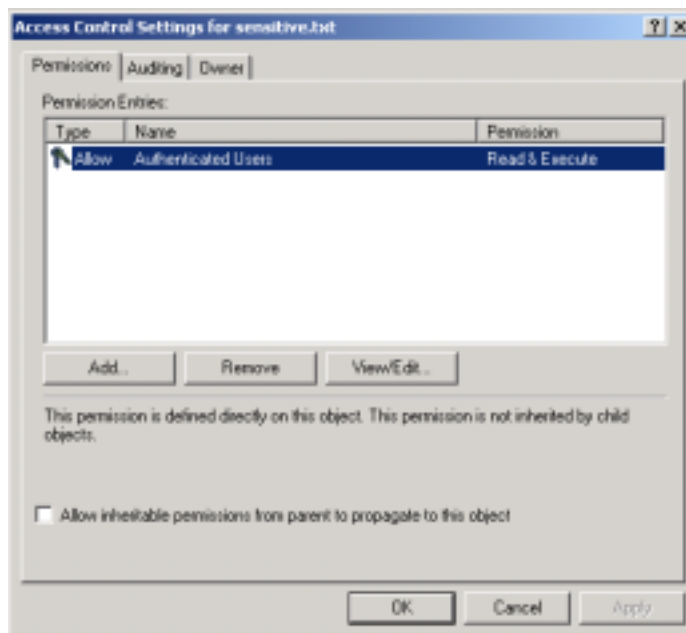
Audit Policy	Description
Audit account logon events	Audits when a user logs on or off a remote computer from this workstation.
Audit account management	Audits when a user account or group is created, changed, or deleted; a user account is renamed, disabled or enabled; a password is set or changed.
Audit 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, printer, and so forth)-that has its own sACL specified.
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 Policy	Description
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

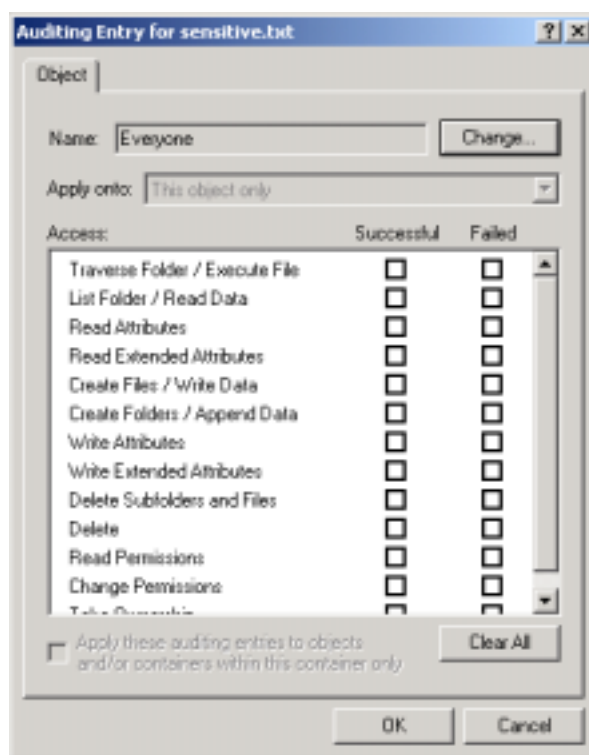
Windows 2000 Professional provides a method to monitor access to any file stored on its NTFS file system. This auditing method is typically used to monitor access to sensitive files. Individual file auditing is configured by right clicking on the file, and then selecting **Properties**. Select the **Security** 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 would like 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 RECCOMENDATIONS

- Apply the NIST template to configure the auditing and event log policies. Refer to the 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 Administrators 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, all patches are applied, and that strong passwords are 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; as such, the common installation steps for Windows 2000 Professional installs will not be discussed. If further information about these steps is required, please 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 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 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.

Windows 2000 introduced a new version of NTFS, called NTFS 5, which has built in support for managing a number of features, including user accounts and security configurations. Windows NT 4.0 uses an older version of NTFS so, 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 file allocation table (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 mechanisms like the ACL mentioned in previous sections. Users should format the operating system 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, there may be a functional reason causing 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` directory, must be executed from an account with administrative privileges. The following sequence of steps will convert any Windows partition to NTFS:

1. Open a command prompt.
 - Select **Run** from the **Start** menu, and type **cmd.exe** to open the Windows 2000 command interpreter.
2. 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.
3. Restart the system upon completion.

Note: This conversion will not occur immediately for **%SystemDrive%** because the virtual memory page file could be in use at the time. 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** file from Microsoft using **secedit.exe** as described in section 2.2 before the NIST Windows 2000 Professional security template is applied.

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 you 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 ERD 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 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 will address the recommended methods creating the ERD and the methods of protecting the sensitive data it contains.

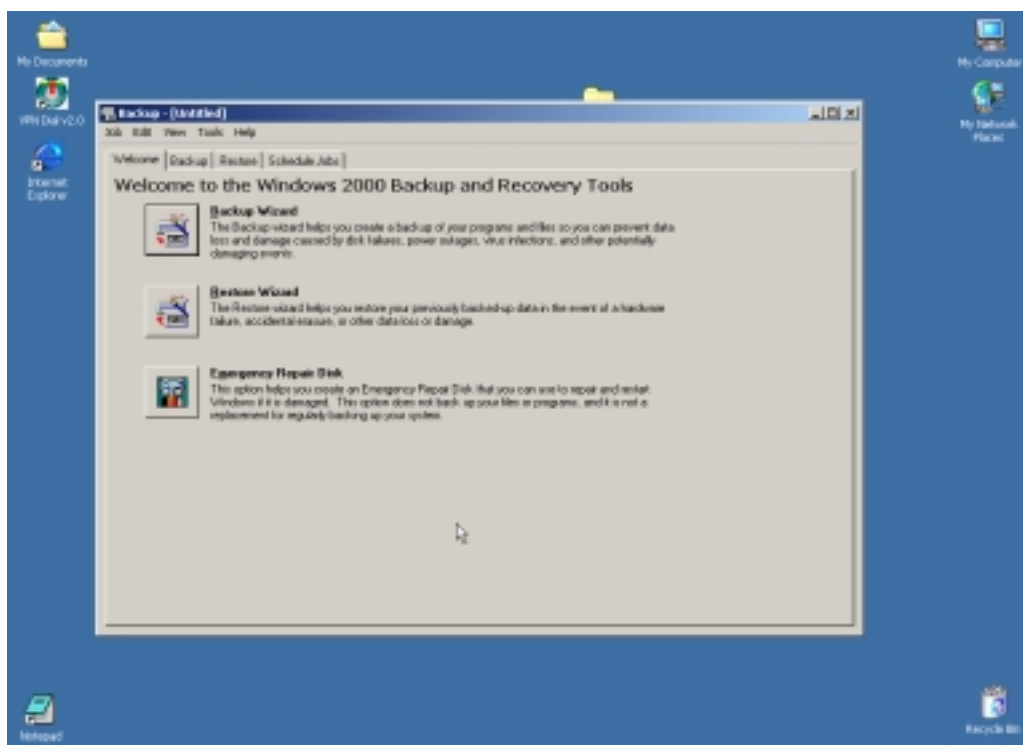
6.4.1 How to Create an ERD

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 the following series of menu commands in sequential order:

Start | Programs | Accessories | System Tools | Backup

This will open the **Backup and Recover 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.

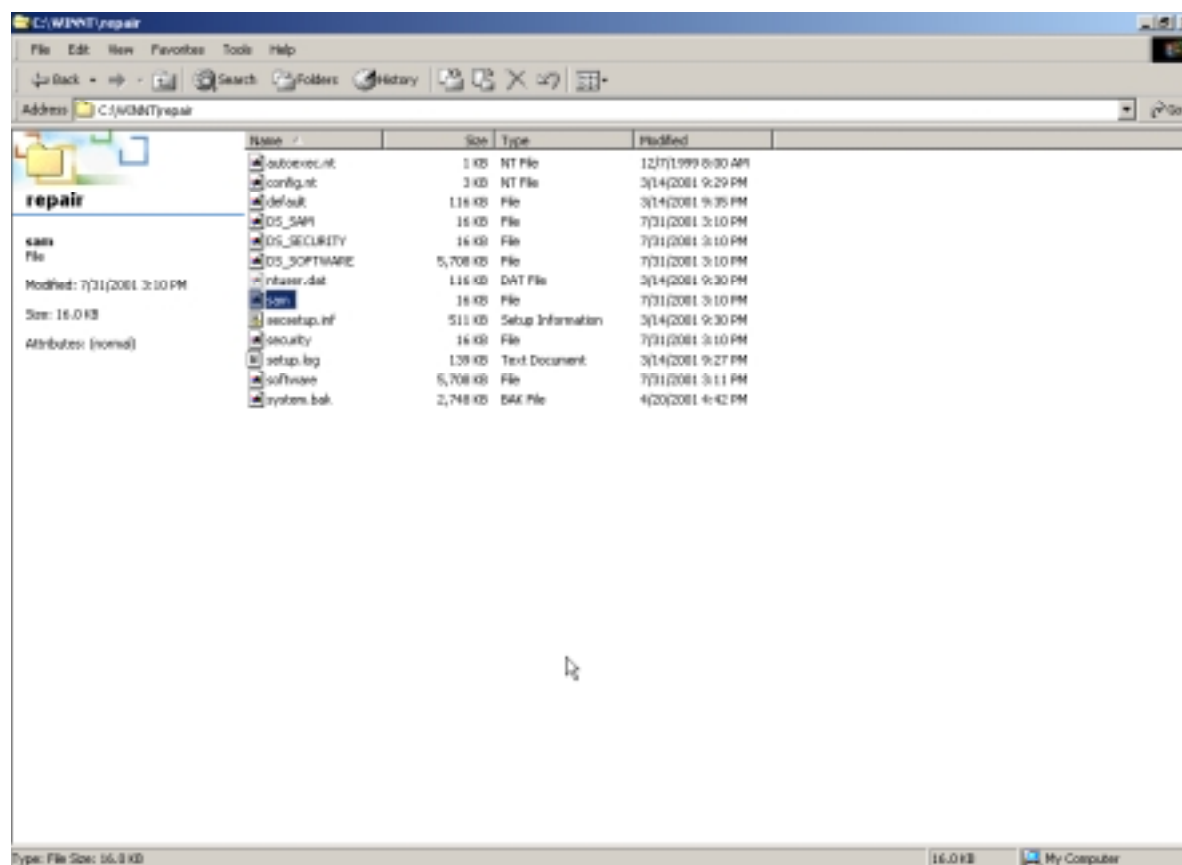
6.4.2 How to Protect ERD

Because the ERD is necessary to repair vital parts of the Windows 2000 Professional operating system, it contains information that must be protected to ensure system integrity. When an ERD is created, a copy of the security accounts manager (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, they 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 such as 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. Included in the contents of the backup ERD is an additional SAM file as shown in Figure 6-2.

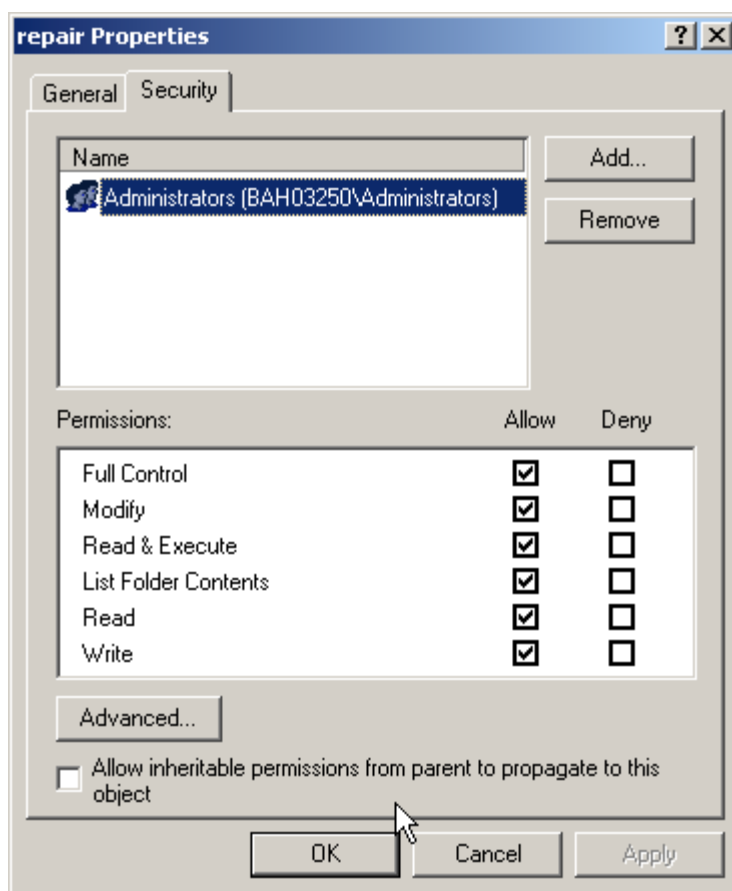
Figure 6-2 Backup ERD showing SAM file



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 of 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, they 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

1. Partition the Hard Drive using NTFS for system and data files.
2. Install OS with minimum required services.
3. Install **Internet Protocol (TCP/IP)** networking and **Client for Microsoft Networking** only.
4. Secure the **winnt\repair** directory. The NIST security template does this automatically.
5. Create the ERD when security configuration is complete.
6. Securely store the ERD on removable media.
7. Delete or restrict access to the backup ERD from the **winnt\repair** directory.

7. UPDATING AND PATCHING GUIDELINES

Windows 2000 Professional users have two main methods to update Windows systems; service packs or hot fixes. The Windows service pack provides improvements and replacements to operating system components. Security updates and hot fixes 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, please refer to **NIST Special Publication 800-40 Applying Security Patches**, available at:

<http://csrc.ncsl.nist.gov/publications/drafts.html>

7.1 WINDOWS 2000 PROFESSIONAL UPDATES

Microsoft publishes updates to the Windows operating system in the form of service packs and hot fixes. The service packs and hot fixes can be obtained in two ways: downloading from the Internet, and ordering a CD containing the files. The latest (SP2) service pack may be downloaded from the following URL:

<http://www.microsoft.com/windows2000/downloads/servicepacks/sp2/default.asp>

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

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

Note: Microsoft provides a command line tool to automate the process of determining the hot fixes required for your computer. This tool is called **hfnetchk.exe** and is located at <http://support.microsoft.com/default.aspx?scid=kb;EN-US;q303215>. The tool can be used to, locally and remotely, check 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. It 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. It can be downloaded from <http://support.microsoft.com/default.aspx?scid=kb;en-us;Q282784>.

Table 7-1 lists the updates provided in Microsoft's latest (September 2001) service pack for Windows 2000 Professional.

Table 7-1: Articles Describing Bugs Fixed in Service Pack 2

Article ID	URL
Q282522	http://support.microsoft.com/directory/article.asp?ID=KB;EN-US;Q282522
Q282524	http://support.microsoft.com/directory/article.asp?ID=kb;en-us;Q282524
Q282525	http://support.microsoft.com/directory/article.asp?ID=kb;en-us;Q282525
Q282525	http://support.microsoft.com/directory/article.asp?ID=kb;en-us;Q298193

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 Administrative users only.

7.2 WINDOWS 2000 PATCHING RESOURCES

Microsoft has developed numerous ways of distributing fixes and patches for vulnerabilities discovered in the Windows 2000 operating system. Microsoft's own security site and third party organizations commonly referred to as Security Portals; serve as an excellent method of notification upon discovery and publication of a new Windows vulnerability.

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.

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

SecurityFocus	http://www.securityfocus.com
NTBugtraq	http://ntbugtraq.ntadvice.com/
Xforce	http://xforce.iss.net

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.

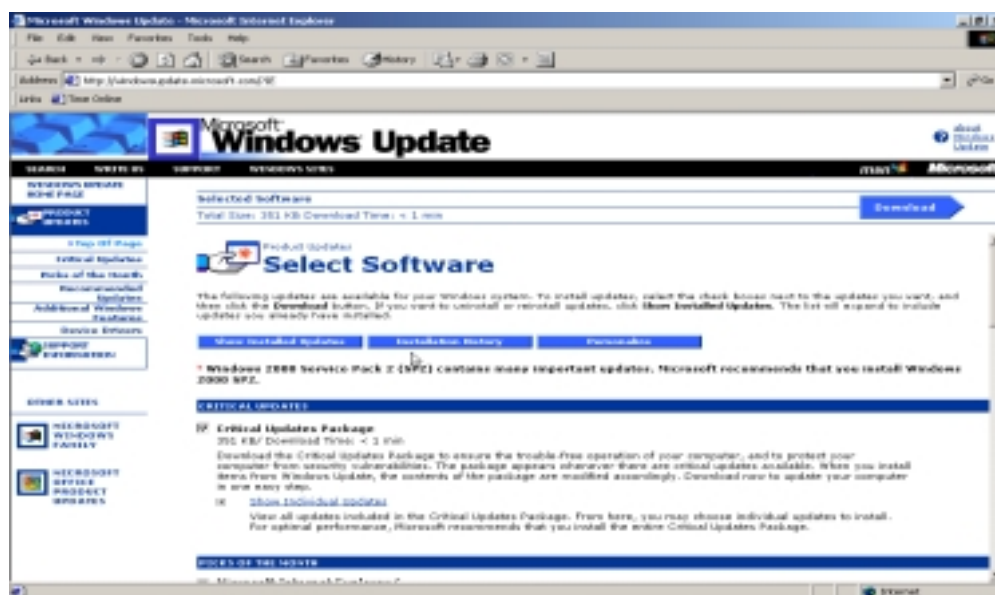
7.2.2 Windows Update Web Site

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 Administrators 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 to 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 that need to be installed. If it finds such updates, the software displays an alert on-screen notifying the user of the situation.

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.

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 Windows 2000 Professional workstation as an on-going 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, there are additional steps that should be taken concerning the file system access control mechanisms that are not included in the installation process. These steps are outlined in this section explaining their importance. The EFS discussed in Section 8.2 is also discussed in detail in this section. 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 on 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 the Windows 2000 Professional machine resides in. The following section provides general information about customizing settings for an environment.

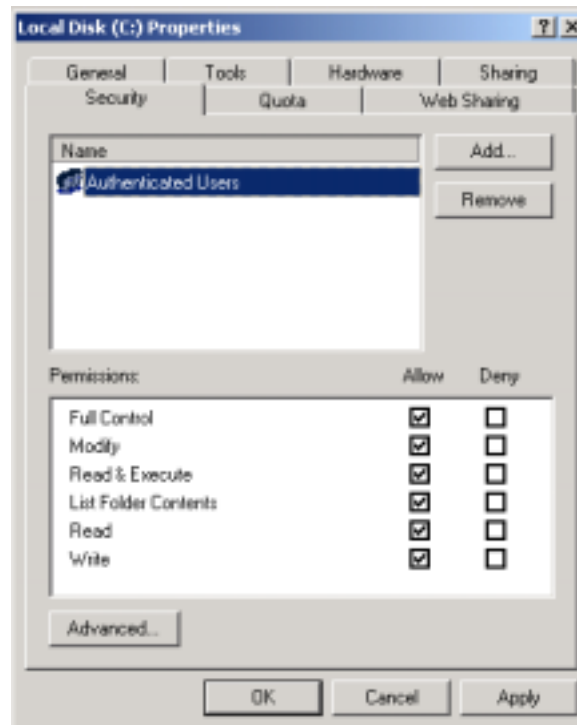
8.1.2 Setting ACLs

Changes to a resource ACL can be made using 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. 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

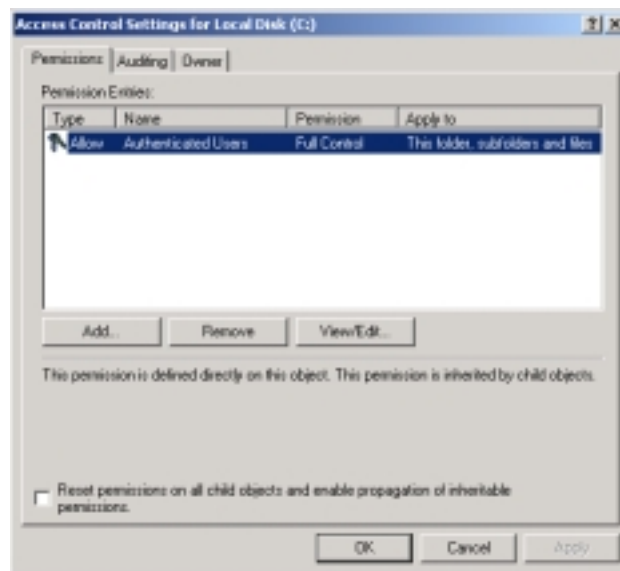
On a Windows 2000 partition, users can set access control lists for specific resources, be it a file or folder, by opening the **Properties** window from that resource's context menu and clicking on the **Security** tab. Figure 8-1 shows a sample ACL. For consistency, each entry that binds a security identifier (SID) to a set of permissions within an ACL is referred to as an ACE.

Figure 8-1: ACL for sample system partition

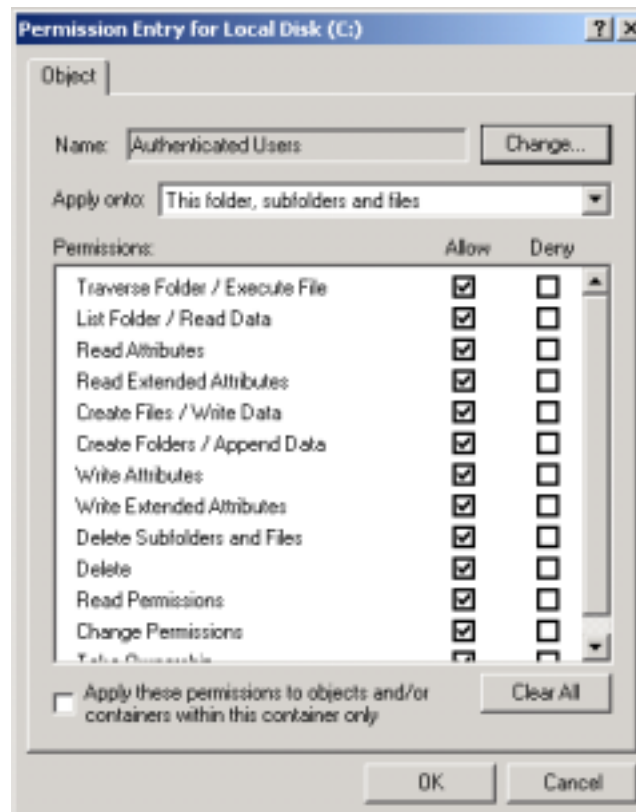


8.1.4 Windows 2000 Access Control

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 is applied before any conflicting inherited ACE.

Figure 8-2: Advanced ACL window for sample system partition

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

8.1.5 Replace Default Access Rights

The examples above used **Authenticated Users** as the default user with full access to partitions. In a default, Windows 2000 Professional, installation the **Everyone** group has access to the directories. It is recommended that the **Everyone** group be changed to **Authenticated Users** group. This will ensure that authentication takes place before any access is allowed to the resource.

The NIST templates provided in Appendix B change the default access on many critical system files. As a rule, remove the **Everyone** group and replace it with the **Authenticated Users** group. Determine if users need full access to the directories within your system and remove the access if it is not necessary. Examples of these critical system files include **boot.ini**, **ntdetect.com**, **ntldr**, **etc**.

Remove access from **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** and **Authenticated Users** only. Examples of these utilities include **rpc.exe**, **regedt32.exe**, **rexec.exe**, **etc**.

8.2 ENCRYPTED FILE SYSTEM

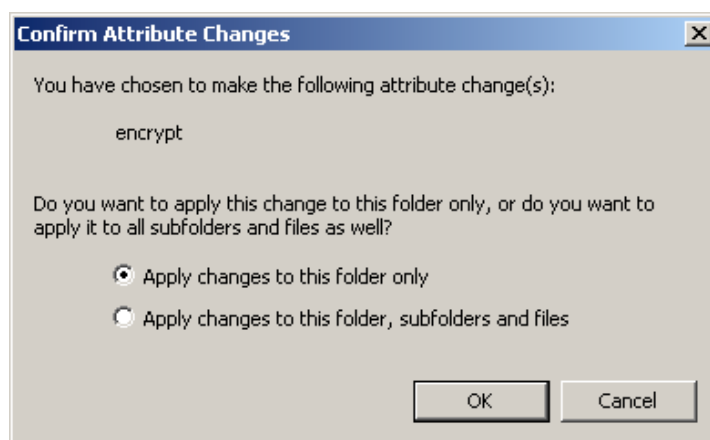
EFS is designed to address a number of concerns regarding the integrity of data stored on secondary storage within Windows 2000. EFS is designed to keep data private and unreadable to unauthorized users. With physical access, malicious users can boot a computer system into a file system other than NTFS effectively bypassing all security provided by NTFS; thus gaining access to all unencrypted files residing on the hard drive of the computer. 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 briefly presented in Section 2.6. The EFS is based on public-key encryption, it 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 is designed to prevent against 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?

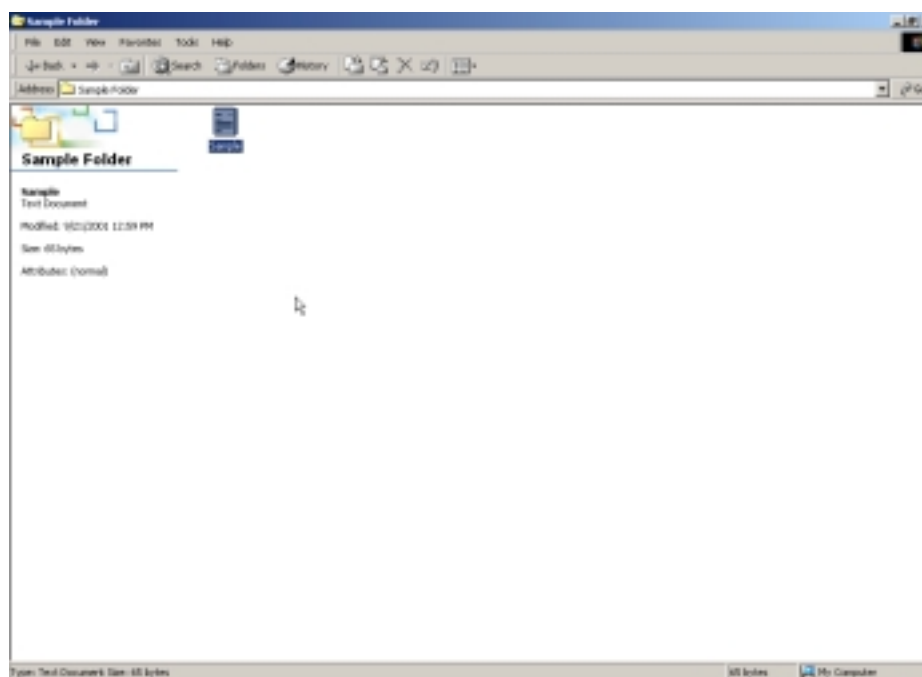
It is recommended that an encryption folder be created for sensitive files. Once a folder is set to encrypt its contents, the user is given the choice to apply this change to every resource within the folder or only apply the attributes to the current folder. The dialog box confirming this attribute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

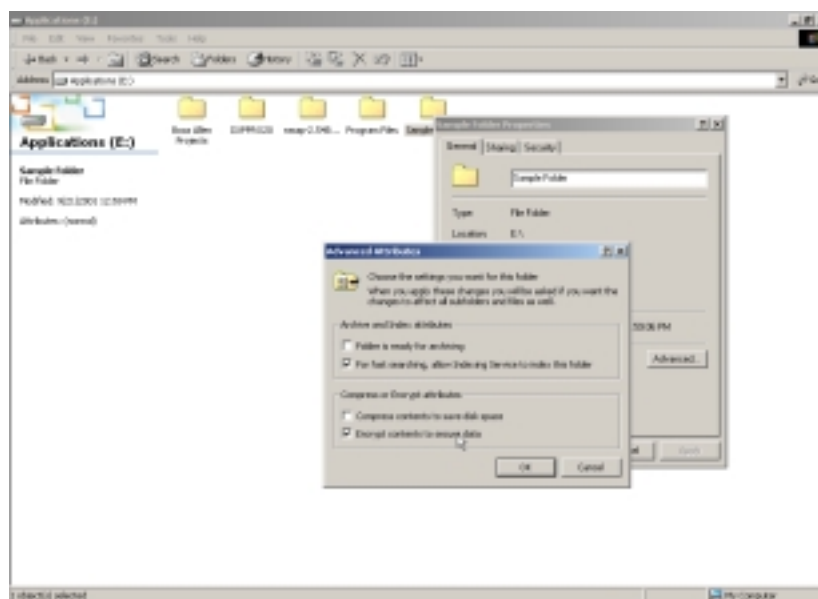
This sample process describes how to implement EFS for a sample folder from within the **My Computer** window. The default configuration of EFS allows a user to encrypt and decrypt files immediately without any administrator interaction. Figure 8-5 shows the directory listing from the **My Computer** 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

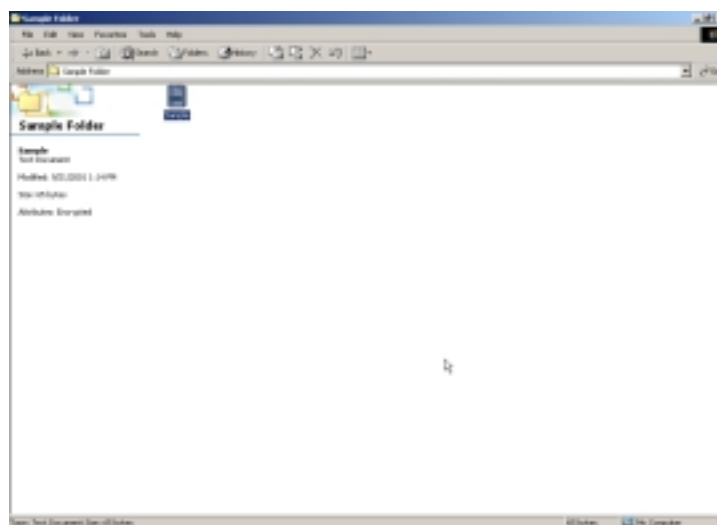
itself, it is recommended that encryption be enabled by opening the **Advanced Properties** window of the folder from one level higher in the directory tree, which frees the user from worrying about individual files. Figure 8-6 shows the **Advanced Properties** window for the folder **Sample Folder**,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

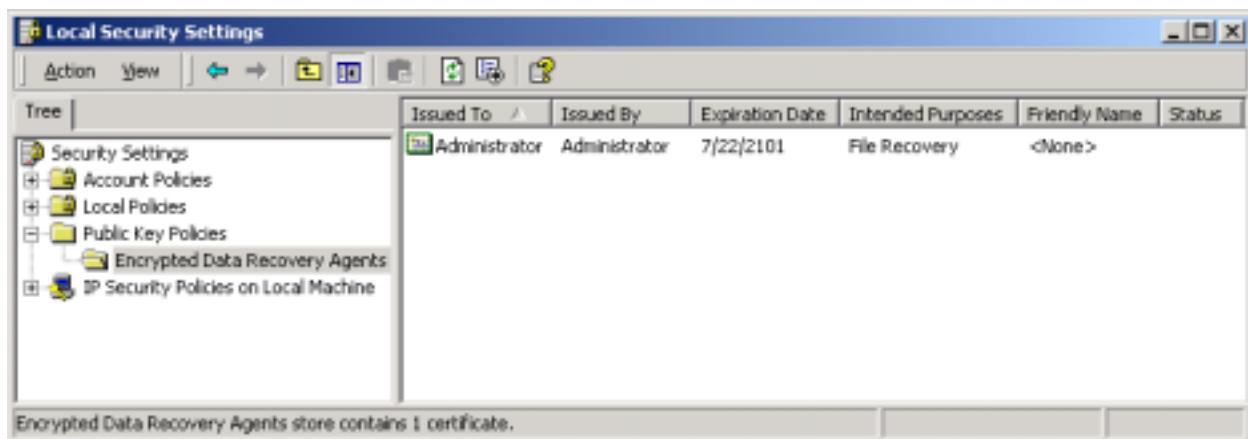
Note: EFS will successfully encrypt files on network shares, yet the data will not be encrypted while in transit. To protect data in transit, a technology such as SSL or IPSec should be implemented.

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, he or she would be unable to access it. This introduces the concept of data recovery. If the owner of the folder or file were to have their 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 ensures that no other private information is revealed to the recovery agent accidentally.

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:

1. Open the **Encrypted Data Recovery Agents** Folder.
2. Right-click the Certificate you would like to export.

3. Choose **All Tasks | Export**.
4. 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 operating system 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 that has been removed from the Recycle Bin by default. 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. The section will review how to remove the 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 operating systems. These features allow application written for these operating systems to be run on a Windows 2000 Professional machine. Since these subsystems can introduce vulnerabilities into a Windows 2000 Professional machine, it is recommended that they be removed.

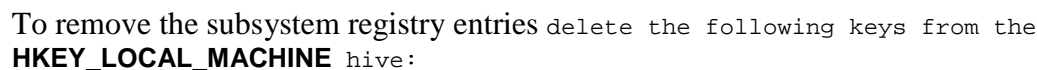
Removing the OS2 and POSIX subsystems is a two-step process: remove the subsystem executables and removing the subsystem registry keys. Windows 2000 Professional stores backup copies of all running system DLLs in the %SystemRoot%\dllcache folder. Successful manual removal of system files requires removal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

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

Figure 8-9: Updated folder listing of Sample Folder



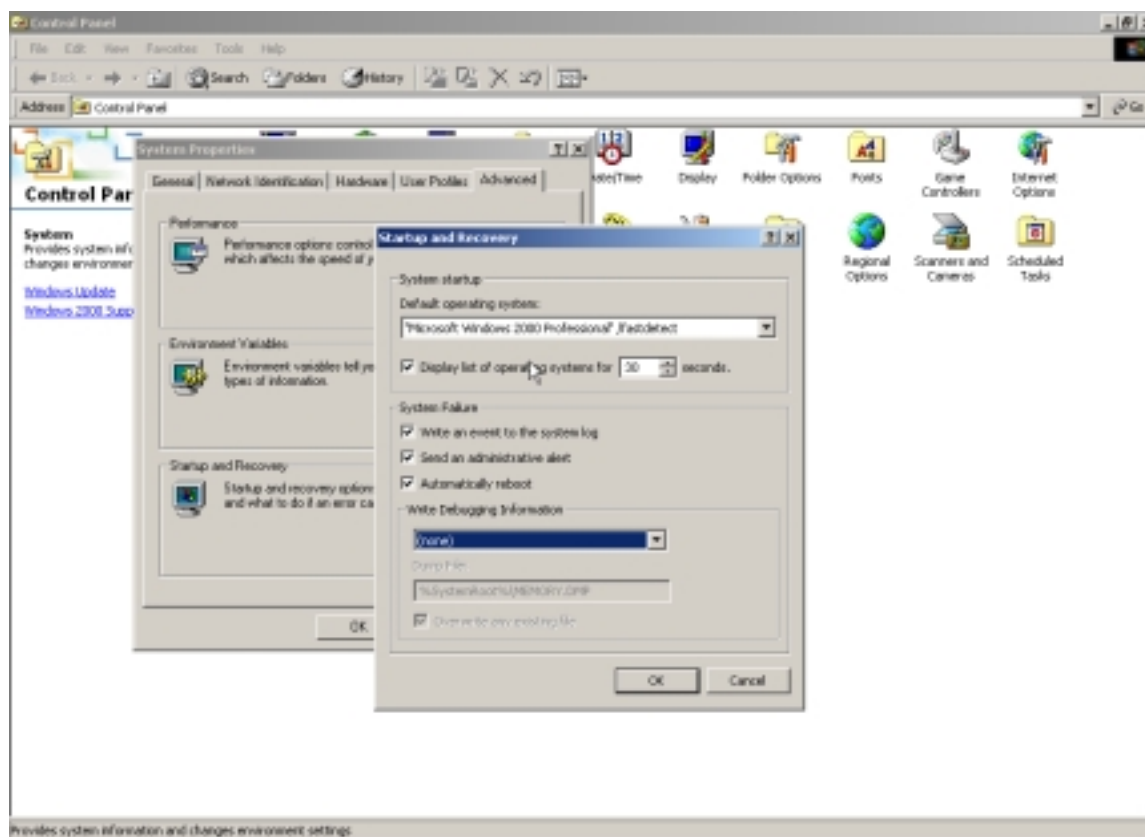
- `\System\CurrentControlSet\Control\Session Manager\Environment\OS2LibPath`
- `\System\CurrentControlSet\Control\Session Manager\Subsystem\Optional`
- `\System\CurrentControlSet\Control\Session Manager\Subsystem\OS2`
- `\System\CurrentControlSet\Control\Session Manager\Subsystem\Posix`

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.

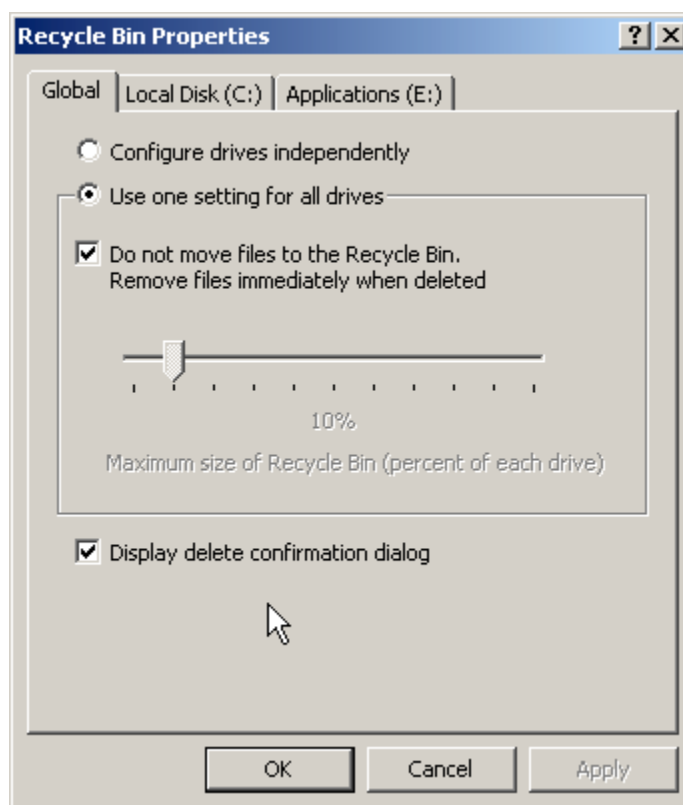
To disable memory dumps on Windows 2000 Professional, open the **System** applet on the **Control Panel**. Once the System applet window is displayed, click on the **Advanced** tab and click the **Startup and Recovery** button at the bottom. This action opens the Startup and Recovery properties window.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

Figure 8-10: Disable operating system memory dumps



NOTE: The Windows 2000 operating system is not the only source of memory dumps! Additional software such as Dr. Watson can create memory dumps in the event of an application error. It is recommended that a user search their hard drive periodically to find and remove any file with an extension of **dmp**.

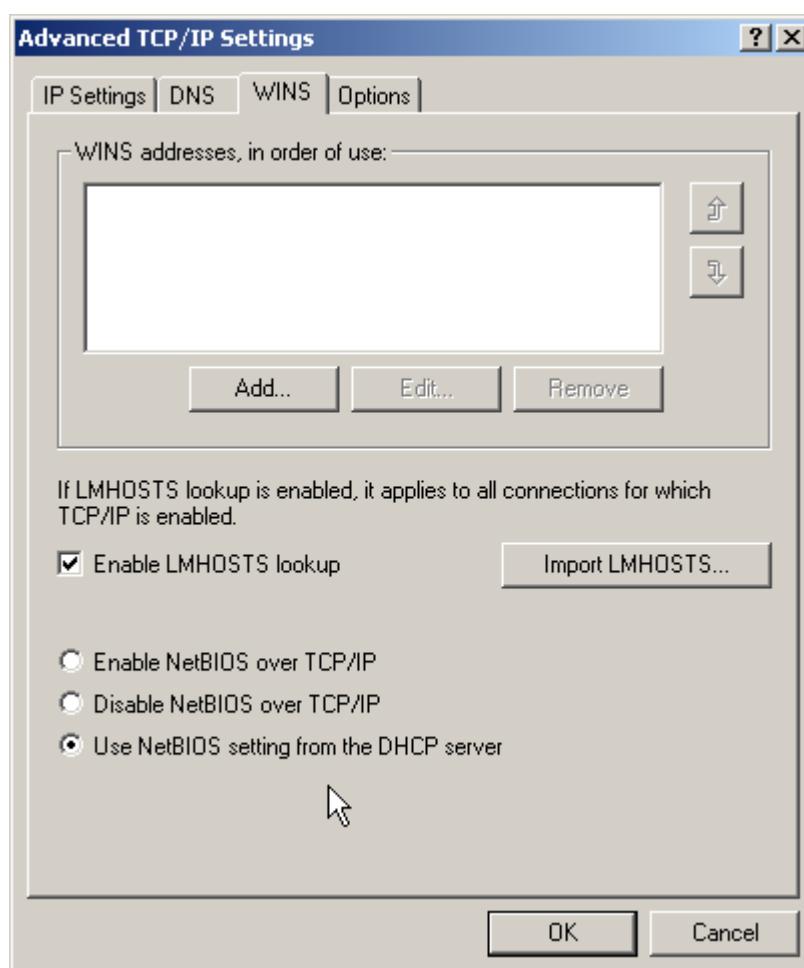
To set the Recycle Bin for immediate deletion of all files, open the recycle bin **Properties** window from its context menu by right clicking on the **Recycle Bin** icon on the desktop. As in the example below, click on the checkbox that says **Do not move files to Recycle Bin. Remove files immediately 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 IDS) should be implemented.

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 DHCP server. If this is true for your network, ensure that the DHCP server assigns connection information that disables this option.

NetBIOS is a non-routable 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, please refer to the **NIST Special Publication Security for Telecommuting and Broadband Communications**. The document is available at: <http://csrc.nist.gov/publications/drafts.html>

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 will allow 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 on site testing to access incoming ports that software installed on the workstation and the network environment the workstation resides in require.

To enable port filtering for a machine, open **Advanced** TCP/IP settings window. Click on the **Options** tab to display additional options for this network connection. Click on the **TCP/IP filtering** option and click the **Properties** button to open the properties window shown in Figure 8-13.

Figure 8-13: Enable TCP/IP Port Filtering

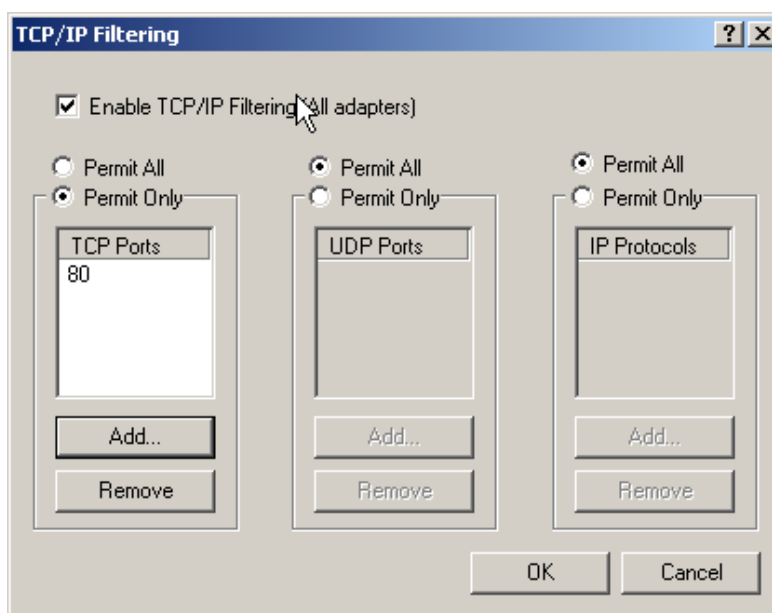


Figure 8-13 presents a scenario with only TCP port 80 allowed access to and from the outside world for HTTP access.

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

To add or edit IPSec filters

1. In **IP Security** policies from the **Local Security Policy** tool, double-click the policy that you want to modify.
2. Double-click the rule that contains the **IP filter list** you want to modify.
3. 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**.
4. In **IP Filter List**, do one of the following:

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, and then click Add .
Reconfigure an existing filter	Double-click the filter.

5. On the **Addressing** tab, select the **Source Address**:

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 <i>Host name</i> . The DNS name is resolved to its IP addresses, and then filters are automatically created for the resolved IP addresses. This option is

	only available when creating new filters.
A Specific IP Address	The IP address that you specify in <i>IP Address</i> .
A Specific IP Subnet	The IP address that you specify in <i>IP Address</i> and the subnet mask that you specify in <i>Subnet Mask</i> .

6. Click **Destination Address** and repeat step 5 for the destination address.
7. Under **Mirrored**, select the appropriate setting:

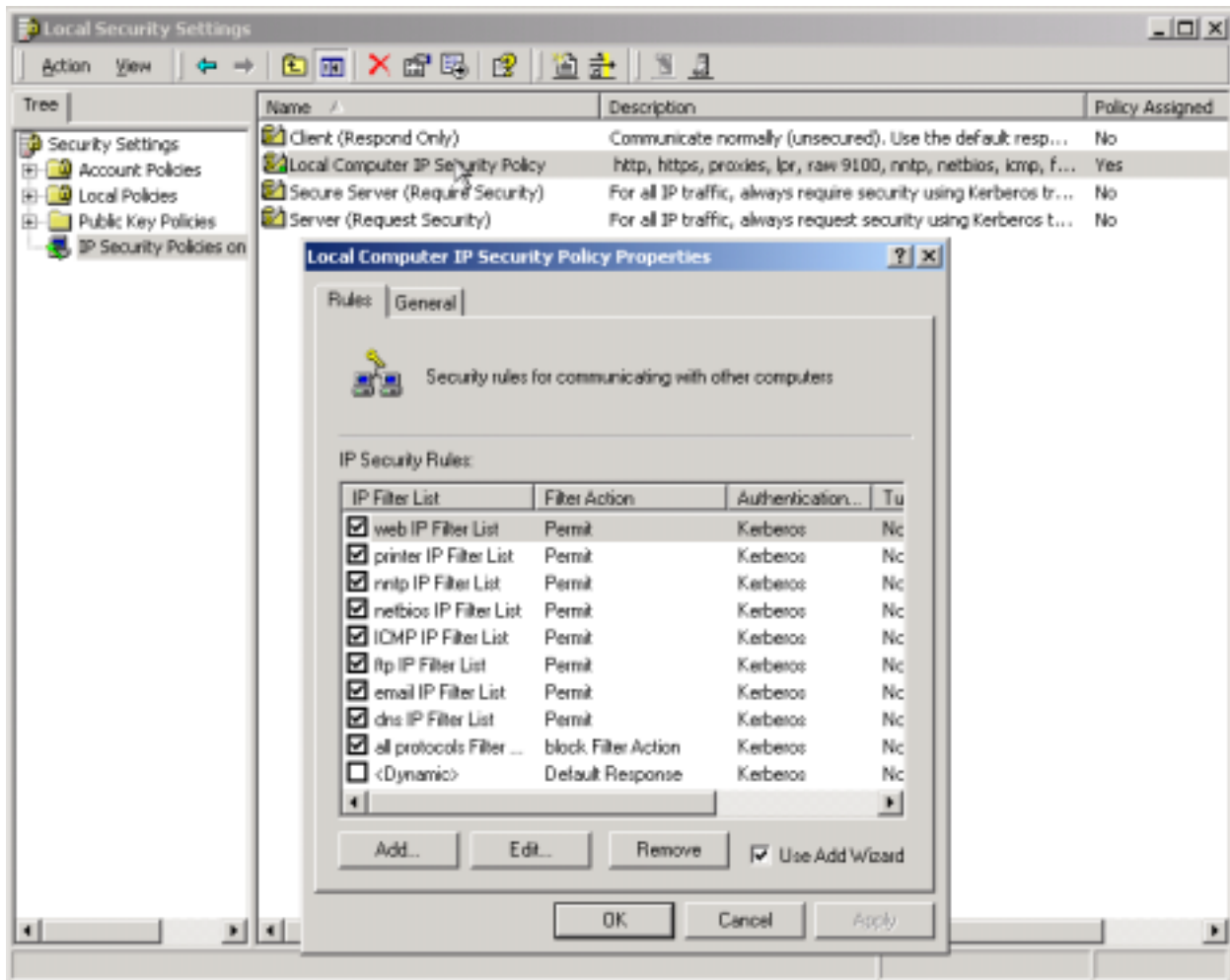
To	Do this
Automatically create two filters based on the filter settings, one for traffic to the destination and one for traffic from the destination	Select the Mirrored check box.
Create a single filter based on the filter settings	Clear the Mirrored check box.
Create a filter for an IPSec tunnel	Clear 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.

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

Figure 8 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 8-14: 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 Manual within the Computer Management MMC snap-in, as shown in Figure 8-15. Disabling a service is a rapid way to stop services from running on a Windows 2000 Professional workstation. Many services cannot be removed entirely and must be disabled. Whenever possible, remove the unneeded services from the system by using the **Add/Remove Programs** control panel.

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 currently is running.

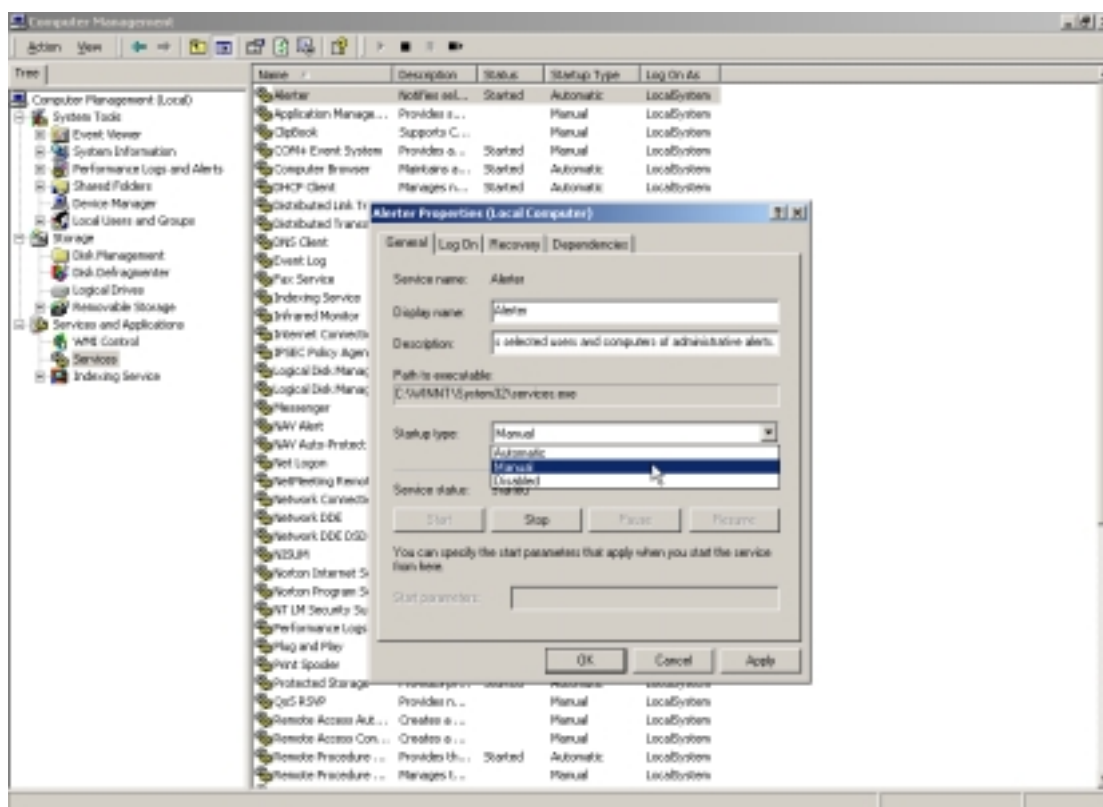
Figure 8-15: Disable unnecessary Services screen

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: Disable Unnecessary Windows 2000 Professional Services

Service	Description
DHCP Client	Responsible for contacting 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. Disable this service if installed programs do not require it.
Server Service	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.
Alerter	Can send a network pop-up 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 only started when a disk is configured or partitioned it is used to provide Administrative functions for Logical Disk Manager. Do not disable if dynamic disks are in the system.
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) Locator	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 in play smart card readers. Disable if no non-plug in play readers will be installed on the system.
Uninterruptible Power Supply	Manages serial communications with an UPS. Disable if not required.
Windows Management Instrumentation (WMI)	Provides system management information used by internal and external partners. Disable this service if access to management information is not required.
Windows Management Instrumentation 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 Applying the Security Template

The security template **NIST2kws.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 insure all settings provided by the **NIST2kws.inf** template are appropriate for their specific environment. Copy the **NIST2kws.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 lab 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\NIST2kws.sdb /cfg C:\winnt\security\templates\NIST2kws.inf
```

This syntax, entered on one line, will apply the security settings specified in the security template **NIST2kws.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. It is important to note that the same task can be achieved using the **Security Configuration and Analysis MMC** snap-in as 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 lifecycle of the system. Examples of occasions for backups outside of 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>

8.6 DOMAIN MEMBER MACHINE CONFIGURATION

The principles discussed in this Section should be applied to a Windows 2000 Professional domain members as well as Standalone workstations. The differences between stand-alone and domain member workstations are in the method of authentication and method of security policy deployment.

Windows 2000 Professional domain members will authenticate to a Windows 2000 domain using Kerberos after the **NIST2kdm.inf** security template is deployed. Active directory **Group Policy** is the preferred method of template deployment in a Windows 2000 Enterprise Domain, refer to Section 4.3.

Note: Test the **NIST2kdm.inf** template 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 security features have been designed by default around three groups of users: Administrators, Power Users, and Users. The Windows 2000 Professional Administration model is based on assigning individual users into groups to control the system access rights of those users. This reduces the Windows 2000 Professional administrative burden by classifying large groups of individual 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 is the only resource assigned to the user.

Administrators 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 to this, any custom right that the Administrators do not have by default, they can grant to themselves. Power Users was created to perform basic administrative tasks in a Windows 2000 Professional workgroup environment. The Users group 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.

The purpose of this section is to discuss each default 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. This section also 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 operating system. Windows 2000 compares the principal's SID with the discretionary access control list (DACL) of the resource.

The DACL is more commonly referred to as an access control list (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 ADMINISTRATOR ACCOUNT

In Windows 2000 Professional, the Administrator account 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.
- Install and repair of Windows operating system.

9.3 POWER USERS GROUP

Any application written with a language compiler that is not Windows 2000 compliant is considered a "legacy application." Only Power Users and Administrators can run legacy applications under Windows 2000. Power Users are able to accomplish the following:

- Install and remove applications per computer that do not install system services.
- Customize system-wide resources (for example, System Time, Display Settings, Shares, Power Configuration, Printers, and so forth).
- 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

File System Object	Default Power User Permissions	Default User Permissions
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 (Files)	RX
%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

File System Object	Default Power User Permissions	Default User Permissions
	RX (Files)	
%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 then illustrates two important and additional steps to take concerning User level accounts:

1. All end-users of Windows 2000 Professional should belong to the Users group ONLY.
2. Applications that end-users need to have access to should be deployed having ACL information configured as such.

An account that is a member of the Users group should in theory be able to run any application that was installed previously by an Administrator, Power User, or other user. This does not turn out to be the case in practice for legacy Windows applications because these applications were designed under a previous version of the Windows kernel and without considering such operating system security. The default permissions for Users are more easily described as follows: users are explicitly granted Write access to the locations specified in Table 9-2 below.

Table 9-2: Users' Write Access Locations

Object	Permission	Comment
HKEY_Current_User	Full Control	User's portion of the registry.
%UserProfile%	Full Control	User's Profile directory.
%Windir%\Temp	Synchronize, Traverse, Add File, Add Subdir	Per-Machine temp directory. This location is for service-based applications so that Profiles do not need to be loaded in order to get the per-User temp directory of an impersonated user.
\ (Root Directory)	Not Configured during setup	Not configured during setup because the Windows 2000 ACL Inheritance model would impact all child objects.

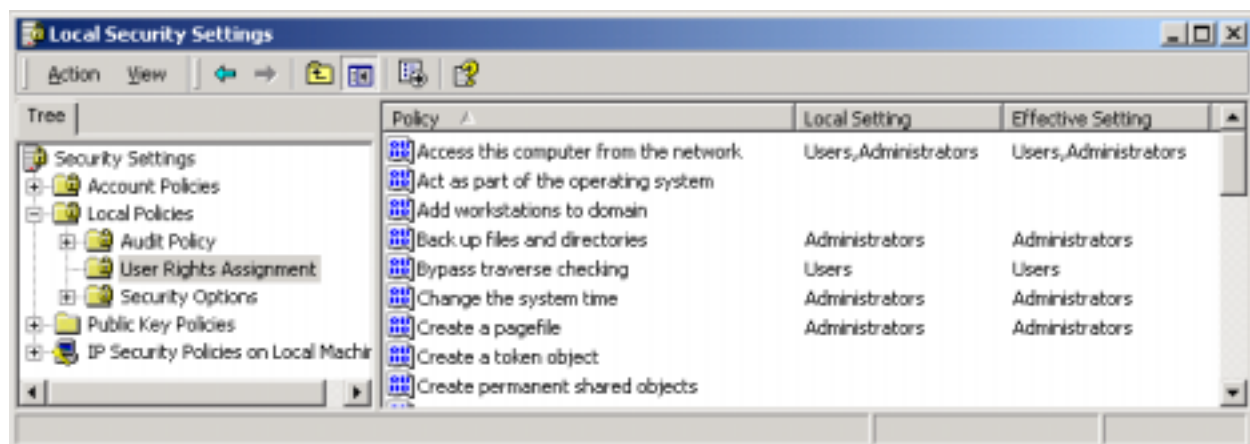
By default, Users have Read (or less) access to the remainder of the system. The default User rights for clean-installed workstation are defined in Table 9-3 below. The settings listed below can be modified in the **Local Security Policy** node under **User Rights Assignment** as shown in Figure 9-1.

Table 9-3: Default User Rights

Policy Description	Setting
Access this computer from the network	Administrators, Backup Operators, Power Users, Users, Everyone
Act as part of the operating system	
Add workstations to domain	
Back up files and directories	Administrators, Backup Operators
Bypass traverse checking	Administrators, Backup Operators, Power Users, Users, Everyone
Change the system time	Administrators, Power Users
Create a pagefile	Administrators
Create a token object	
Create permanent shared objects	
Debug programs	Administrators
Deny access to this computer from the network	
Deny logon as a batch job	
Deny logon as a service	

Deny logon locally	
Enable computer and user accounts to be trusted for delegation	
Force shutdown from a remote system	Administrators
Generate security audits	
Increase quotas	Administrators
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators
Lock pages in memory	
Log on as a batch job	
Log on as a service	
Log on locally	Administrators, Backup Operators, Power Users, Users
Manage auditing and security log	Administrators
Modify firmware environment values	Administrators
Profile single process	Administrators, Power Users
Profile system performance	Administrators
Remove computer from docking station	Administrators, Power Users, Users
Replace a process level token	
Restore files and directories	Administrators, Backup Operators
Shut down the system	Administrators, Backup Operators, Power Users, Users
Synchronize directory service data	
Take ownership of files or other objects	Administrators

Figure 9-1: User Rights Assignment



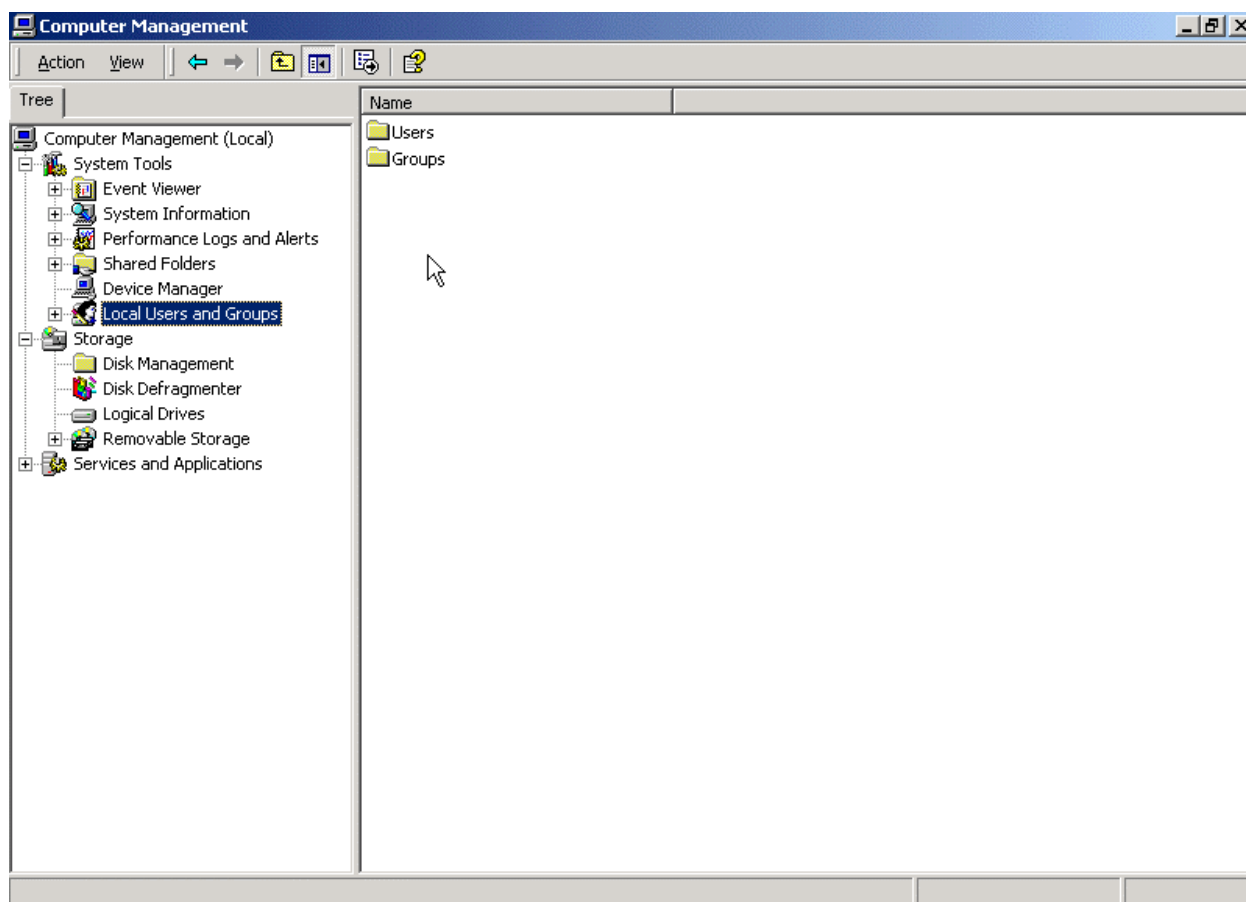
9.5 CHANGE ACCOUNT GROUP MEMBERSHIP

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.

As stated in the introduction, three default groups of users are included with Windows 2000 Professional out of the box: Administrator, Power User and User. There are actually six user groups created on installation, but this discussion will only focus on the primary three. 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 9-2.

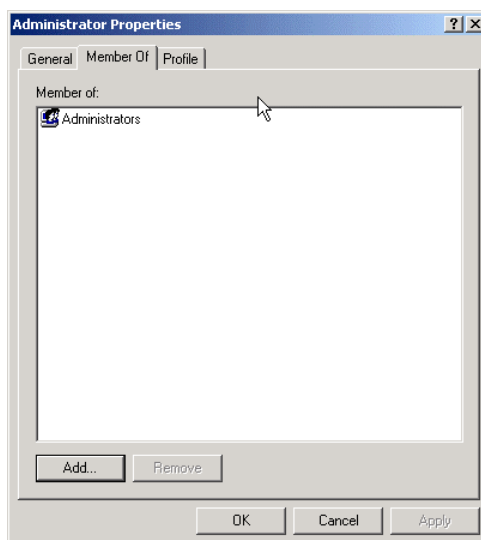
Figure 9-2 Open Local Users and Groups from Computer Management



This action opens the User Management applet, which allows control over the accounts properties. As shown in Figure 9-2, 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 9-3. Double clicking on the specific user icon can open the same properties window.

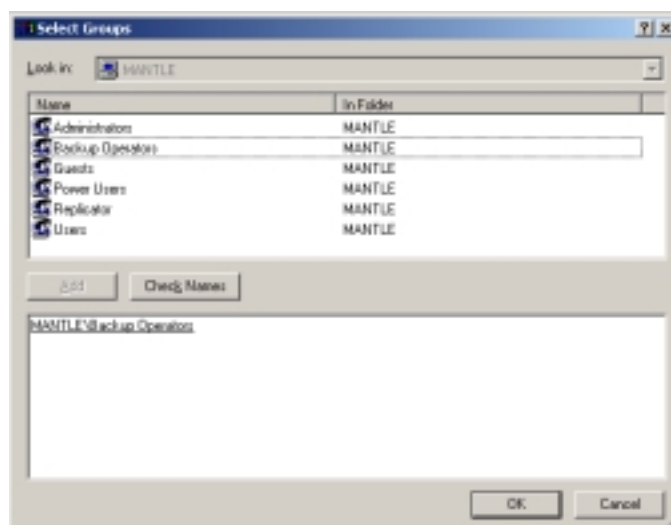
In Figure 9-3 the **Member Of** tab is showing that the user is a member of the Administrators group.

Figure 9-3: 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 and click on the **Add** button, and choose **OK** to close the **Select Groups** Window. Figure 9-4 shows the example user being added to the Backup Operators group.

Figure 9-4: Add user client to Backup Operators group

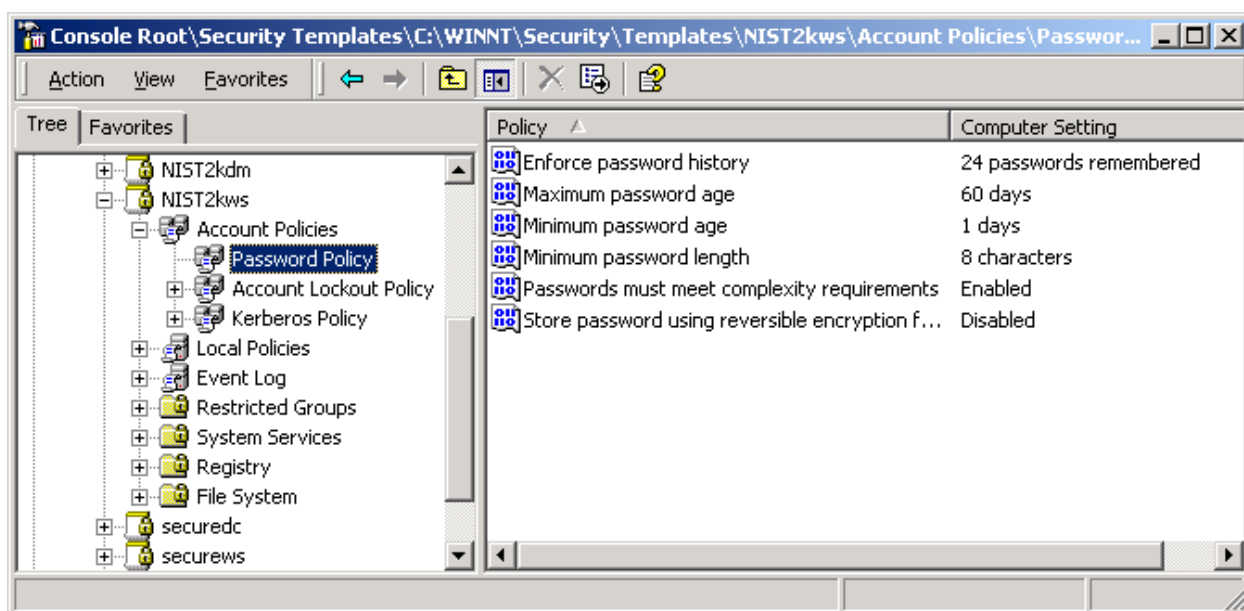


9.6 ACCOUNT POLICIES

The NIST templates contain the NIST recommended password policy settings as shown in Figure 9-5. 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 in length, 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 non-alphanumeric (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 9-5: 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.

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 both in the federal and private sector are discussed. Application configuration tends to involve a number of 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/index.html>.

10.1 ANTI-VIRUS 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 include 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 it 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** – Gives ability to connect to the manufactures site for automatic updates of virus definition files.

Each one of these components is important in its own right, and should not be ignored or 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.

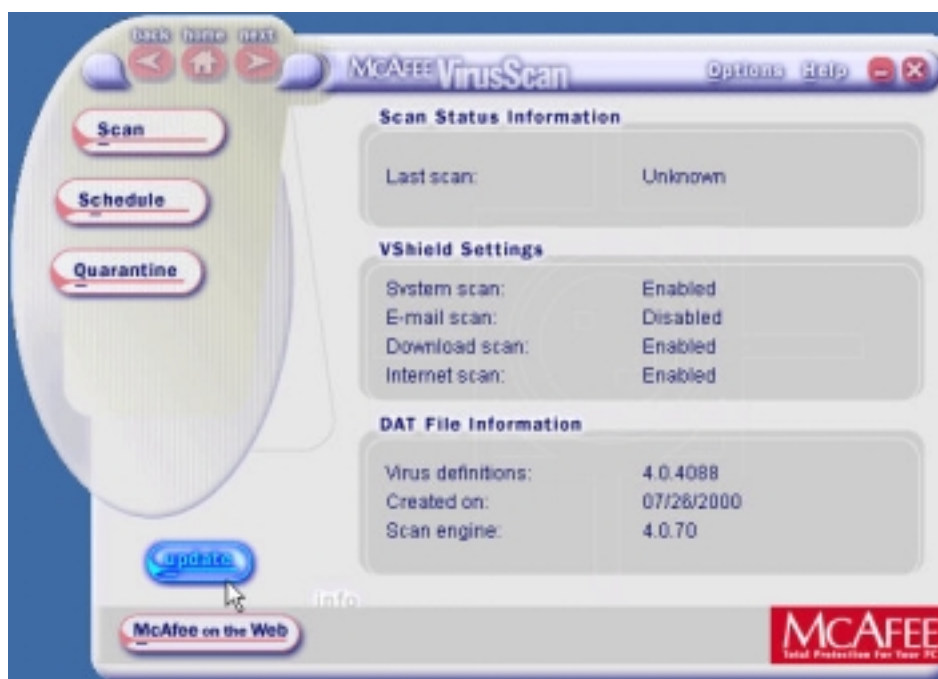
10.1.1 McAfee Virus Scan

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

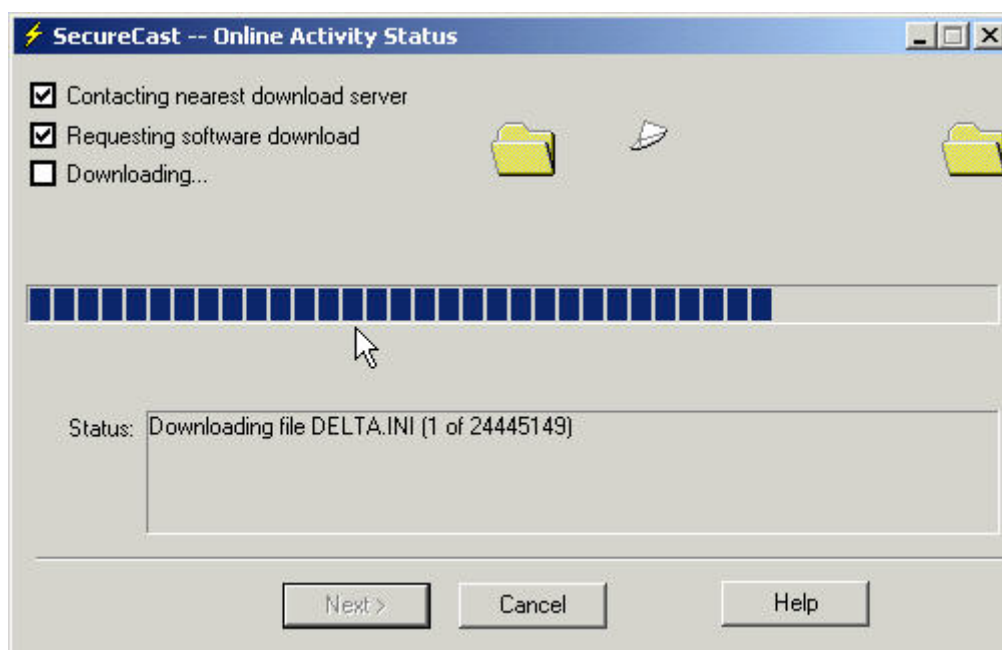
- <http://www.mcafee-at-home.com> - for home users
- <http://www.mcafeeb2b.com> - for corporate users

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 to purchase a CD copy of McAfee, or to purchase online and download from mcafee.com. This discussion will focus on McAfee Virus Scan installed with McAfee Office. The installation process of McAfee is straightforward, but proper configuration is necessary, and this is done 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 anything else is done, including 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

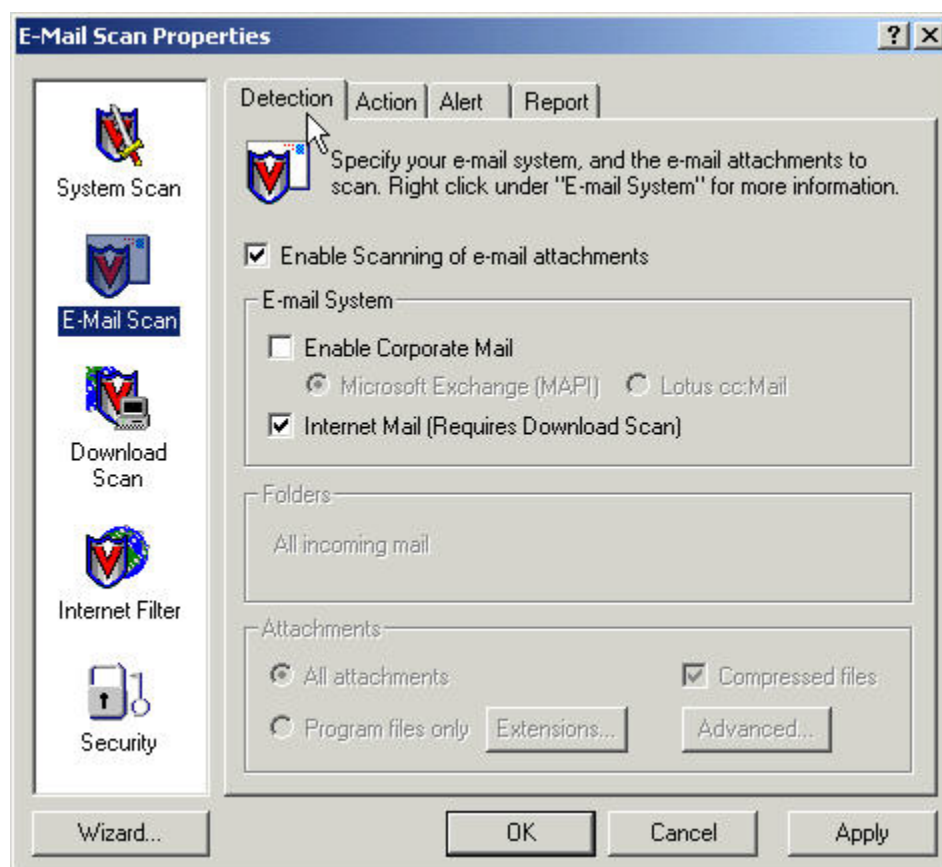
This process starts the update utility SecureCast, which downloads and installs the newest data, files for McAfee as shown in Figure 10-2. SecureCast will not allow updates to McAfee unless proper registration information has been submitted.

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 and click on the **E-Mail Scan** option in the list on the left side.

Figure 10-3: Configure McAfee e-mail scanning



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 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 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

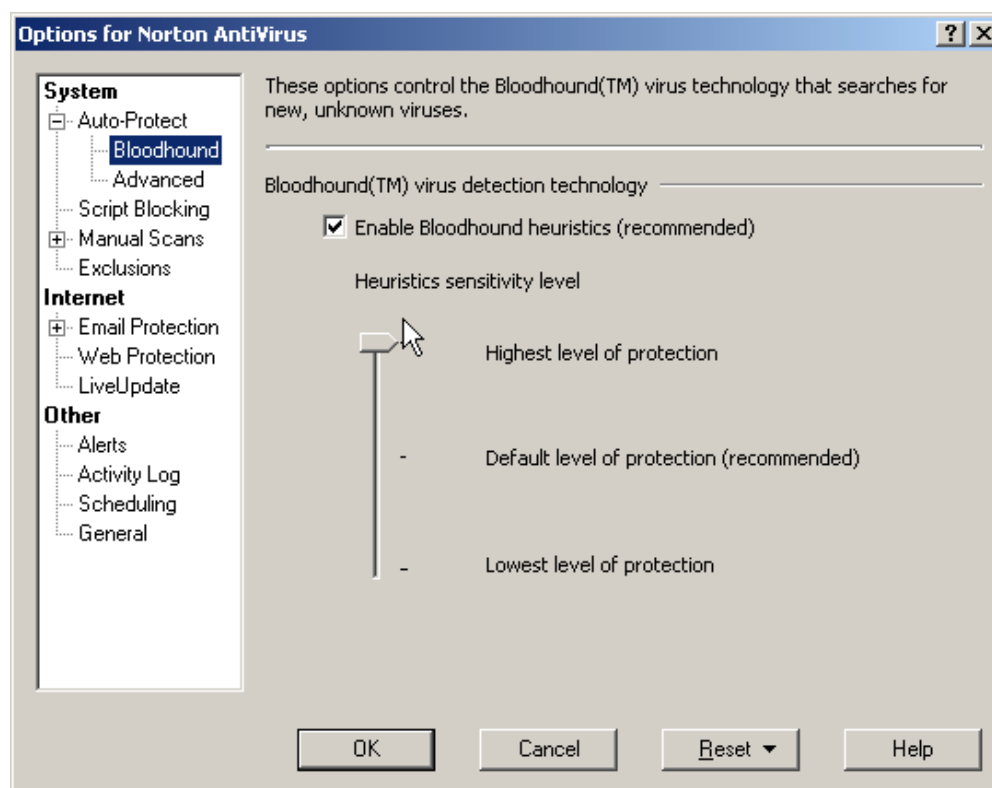
Figure 10-4: Configure McAfee settings password protection

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 only. 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, do the following:

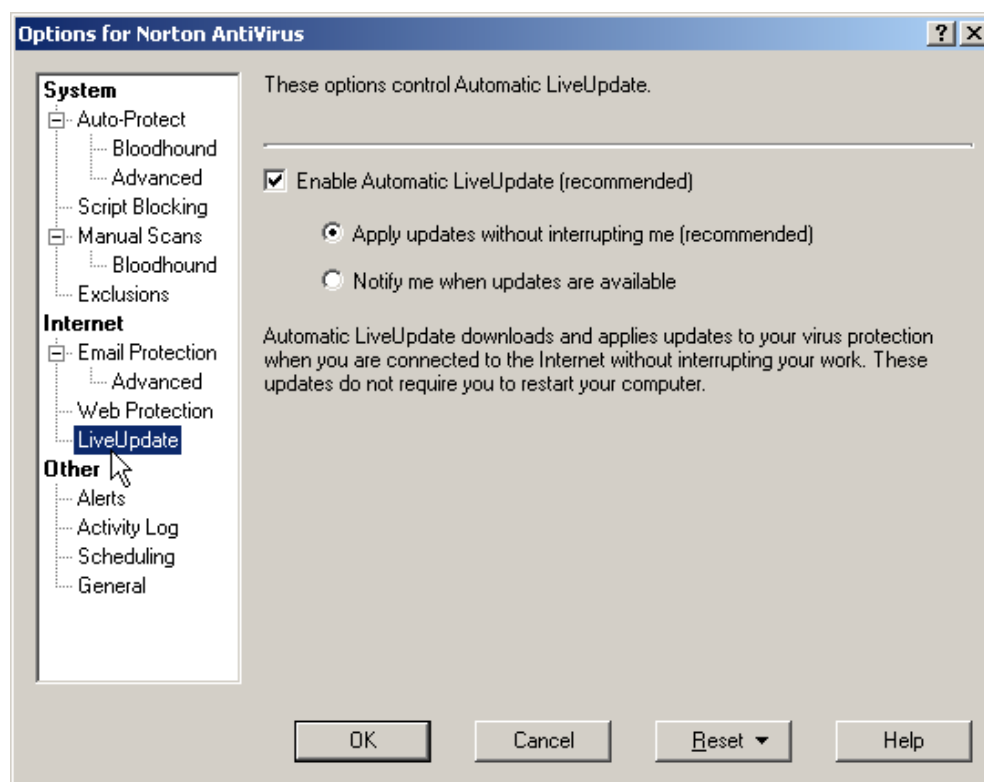
1. Open the **Norton Anti-virus auto-protect** window from the task bar.
2. Click on the **Options** button at the top of the window to open the Norton Anti-virus options.
3. Expand the **Auto-Protect** setting on the left side of the option window and click on the **Bloodhound** choice. Ensure that 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 Anti-virus 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:

1. Open the **Options** screen again as in the previous example.
2. Click on the **Live Update** option.
3. Ensure that the Enable **Automatic Live Update** checkbox is checked.
4. 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 Anti-virus. 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 Anti-virus automatic live update

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

1. Open the Norton options screen as in the previous example.
2. Expand the **E-mail Protection** option.
3. 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 done, 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 is successful, close the options screen and return to the main Norton Anti-virus screen. If the e-mail status option is clicked, Norton should report that Email accounts are protected.

NOTE: The actual binary on the system that scans the messages for Norton AntiVirus stand-alone edition is called **popproxy.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.

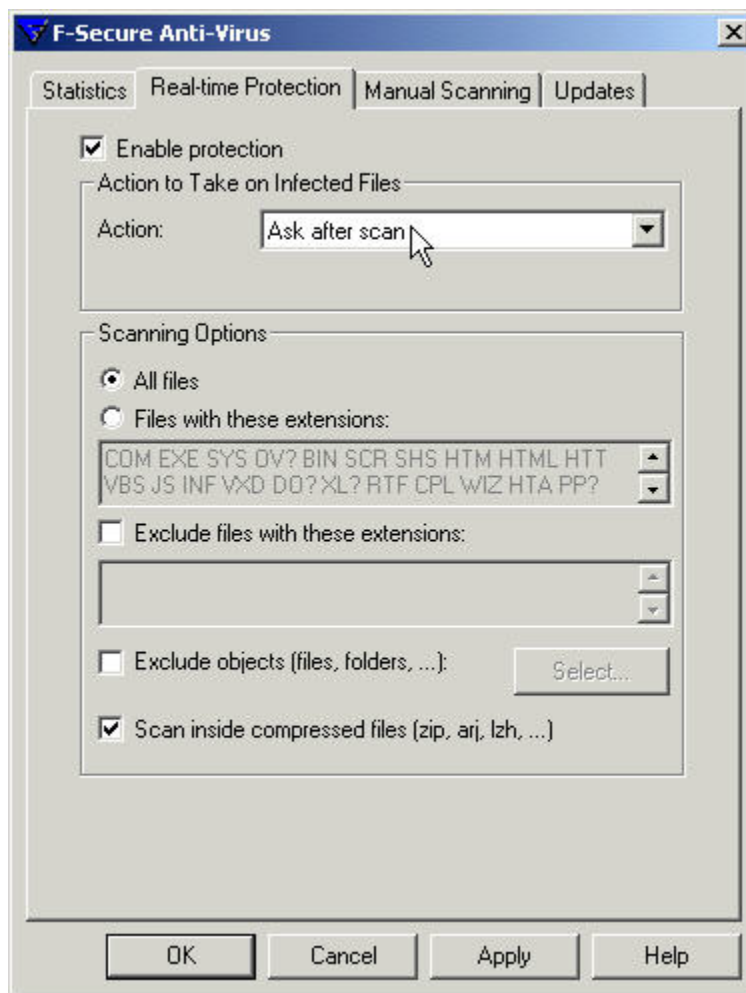
10.1.3F-Secure Antivirus

F-Secure Anti-virus is a product of the F-Secure Corporation and is available online from:

<https://europe.f-secure.com/products/antivirus/>

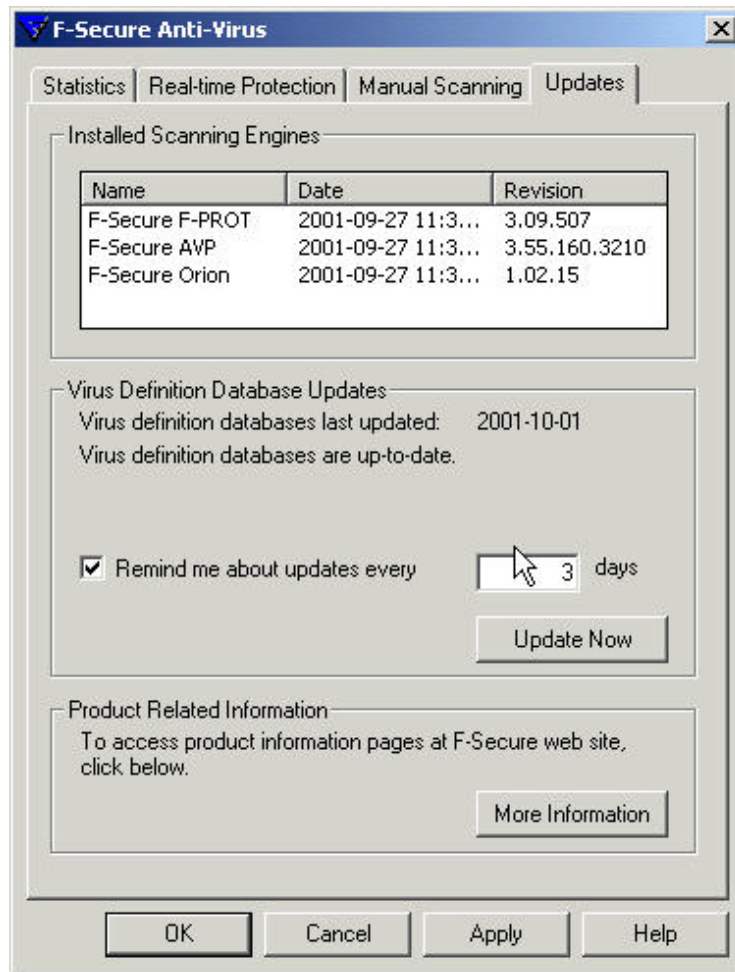
The current version of F-Secure is 5.30, which does not provide any e-mail scanning capabilities. The installation process has no reported problems and can install with default settings provided there is enough space on the partition. Once installed, just as with other antivirus software it is recommended that real-time protection be enabled. To enable real-time protection, double click on the **F-Secure** icon in the System tray. This opens the **F-Secure Anti-Virus** options window shown 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 EMAIL 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 will focus 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 patches the software regularly, restricts the execution of active code, and understands 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 hot fixes 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 the Productivity Application section below.

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 upon which version of Internet Explorer is installed. Ensure that the latest stable version of Internet Explorer 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 provides a user the ability to automate many of the management and repetitive tasks on the Windows 2000 Professional operating system. 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 breakneck speed today, with such a brisk pace, its dangerously easy to open an message with a subject that says "Here is the file you requested" without looking at the sender. These worms can rapidly spread throughout an enterprise or even the entire Internet because of the default interoperability of the Windows 2000 Professional and MS Office.

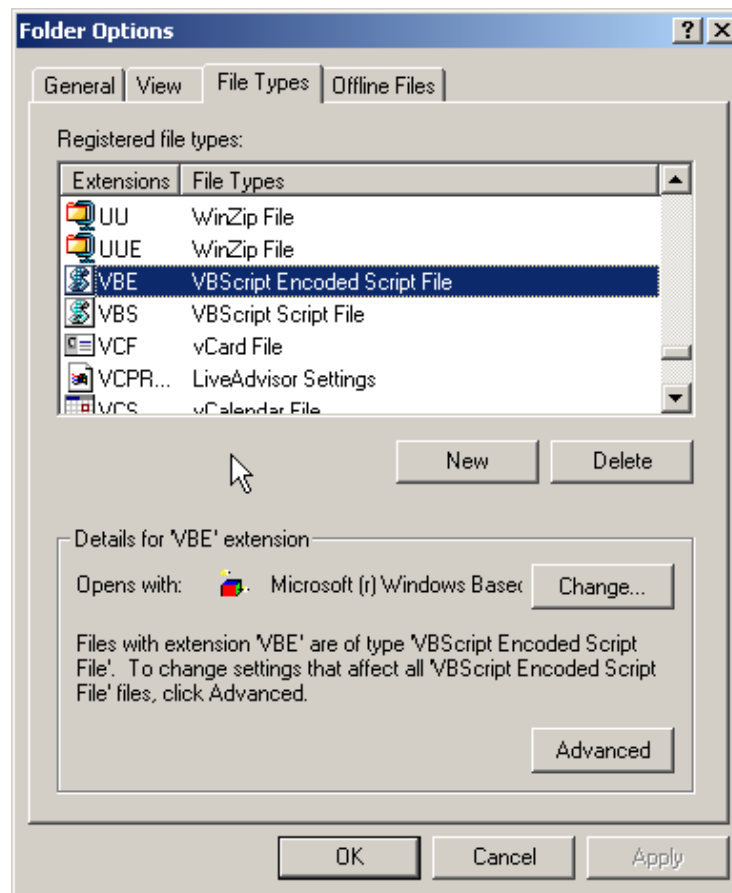
The following paragraphs will focus on the protection of the enterprise and workgroup networks by disabling features that leave Outlook susceptible to malicious code. The recommended method to disable VBS driven malicious code is to follow the steps listed below:

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 the 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 re-inserted 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 curb 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

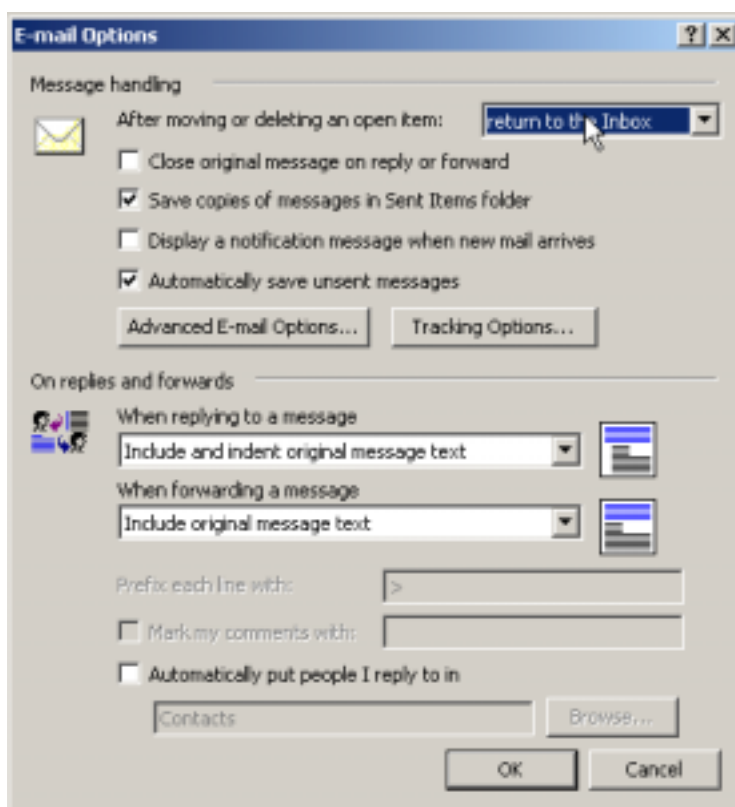
(WSH) and VBS provide. Be sure to be aware of this before removing these associations.

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 drop-down 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



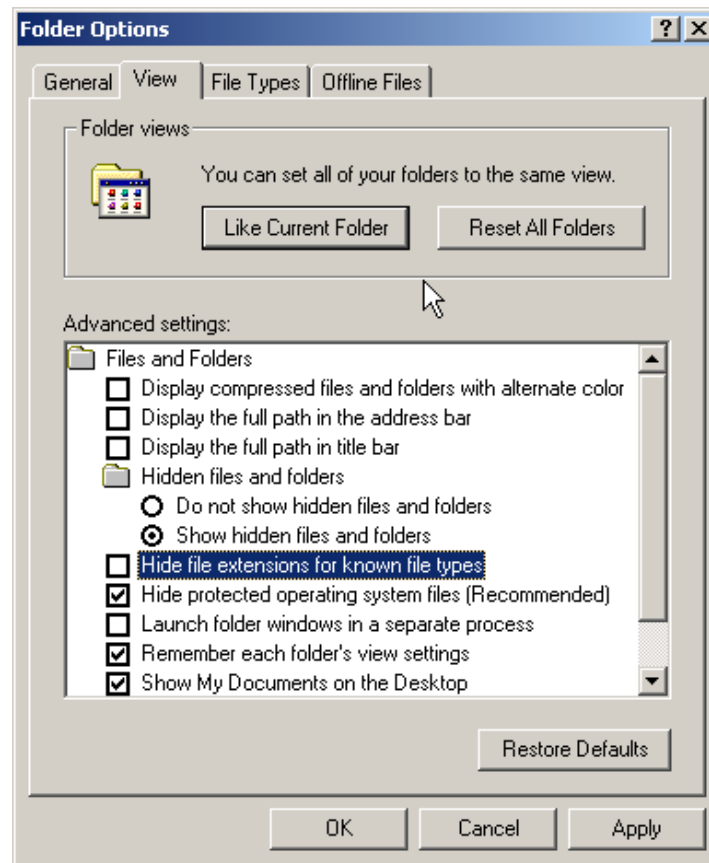
3. Turning off the Outlook preview pane helps to prevent corrupt messages from executing their payload as soon as the message is selected.
 - a. Click on the Microsoft Outlook **View** menu option.
 - b. In the drop-down menu, locate the **Preview Pane** and **Auto Preview** menu option.
 - c. If either 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

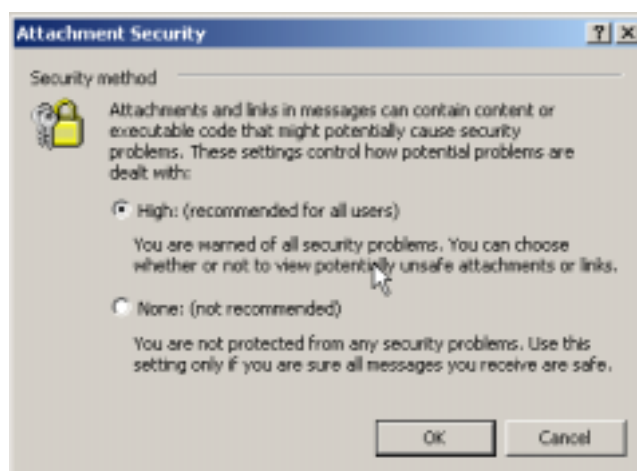


10.2.1.2 Outlook Attachment Security

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 shown in Figure 10-12, ensure that this setting is set on **High Security** and close the window.

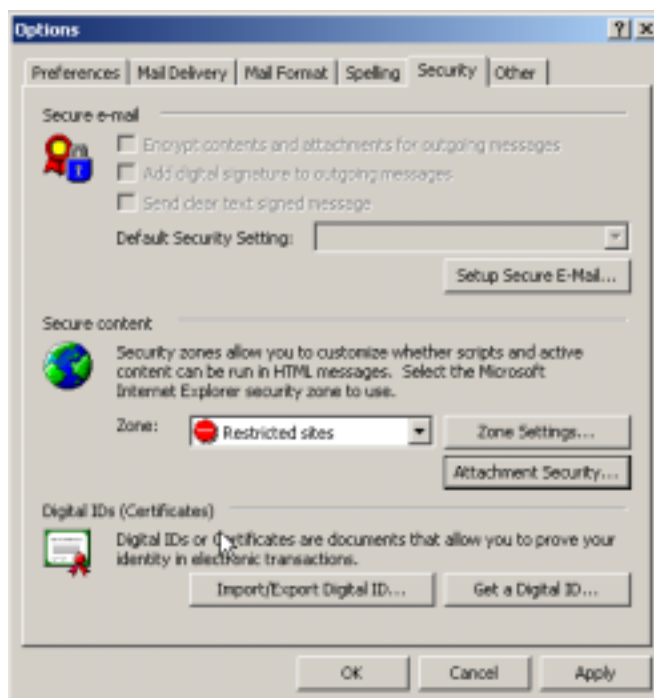
Figure 10-12: Set Outlook Attachment Security to High



Also on the security **Options** tab, users are recommended to 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 is currently working to resolve, <http://support.microsoft.com/default.aspx?scid=kb;EN-US;q277704>.

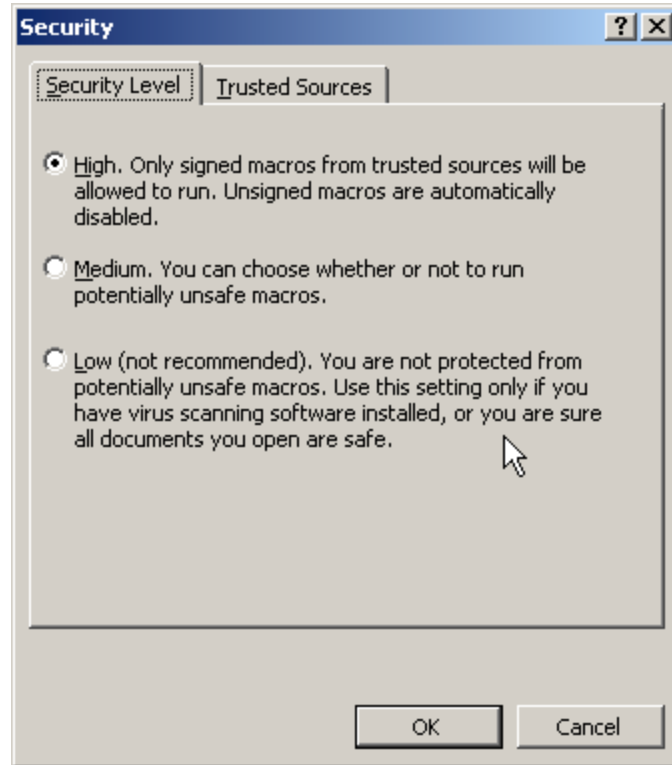
Figure 10-13: Set Outlook Security Zone



Users are also recommended to 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.
2. Set the **Security Level** to **High**, as shown in Figure 10-14.

Figure 10-14: Set Outlook Macro Security

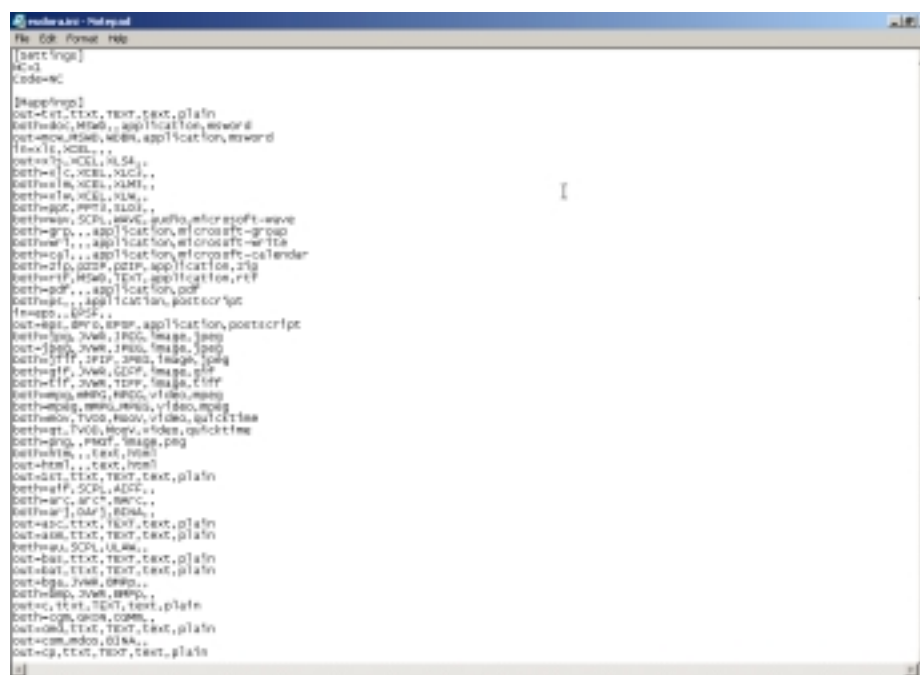


10.2.2 Qualcomm Eudora

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/>

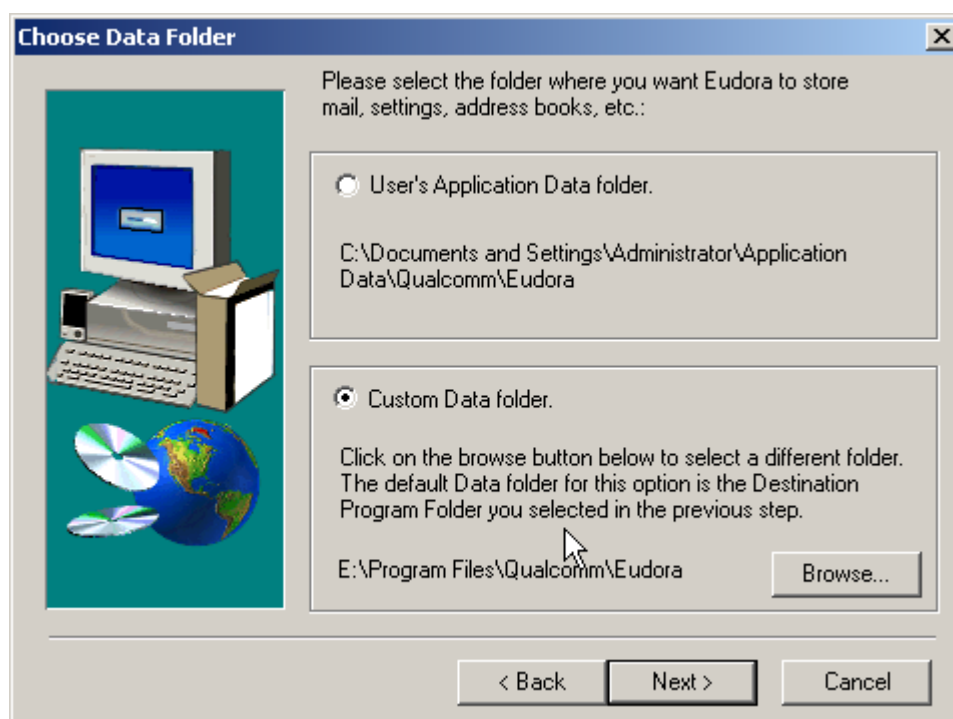
Malicious active content transmitted via e-mail messages is also a concern to Eudora. Just as Microsoft Outlook does, Eudora can warn a user about interacting with file based on the file extension. Eudora is configured to alert users with a dialog box when they are about to open a file with a registered 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 below.

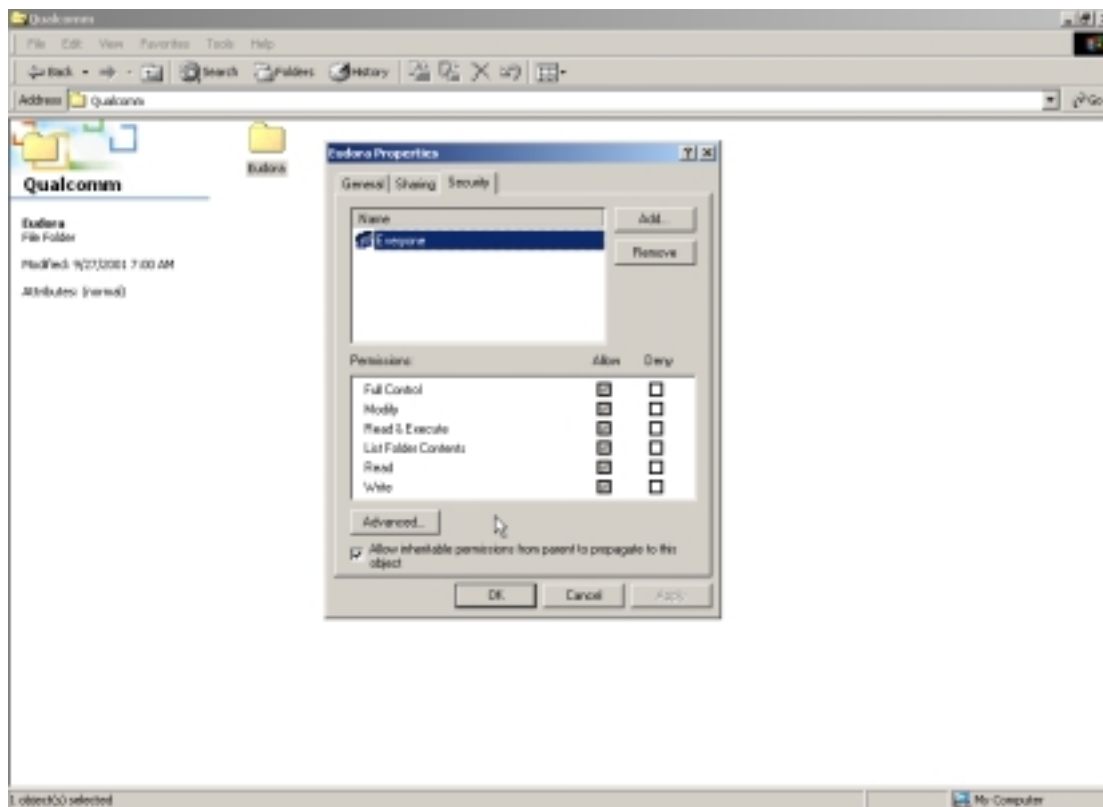
Figure 10-16: Choose where to install Eudora data files



This is a critical step in the installation process. Here, this user has chosen to install the data files into the same directory that the Eudora program was chosen to install in. This 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



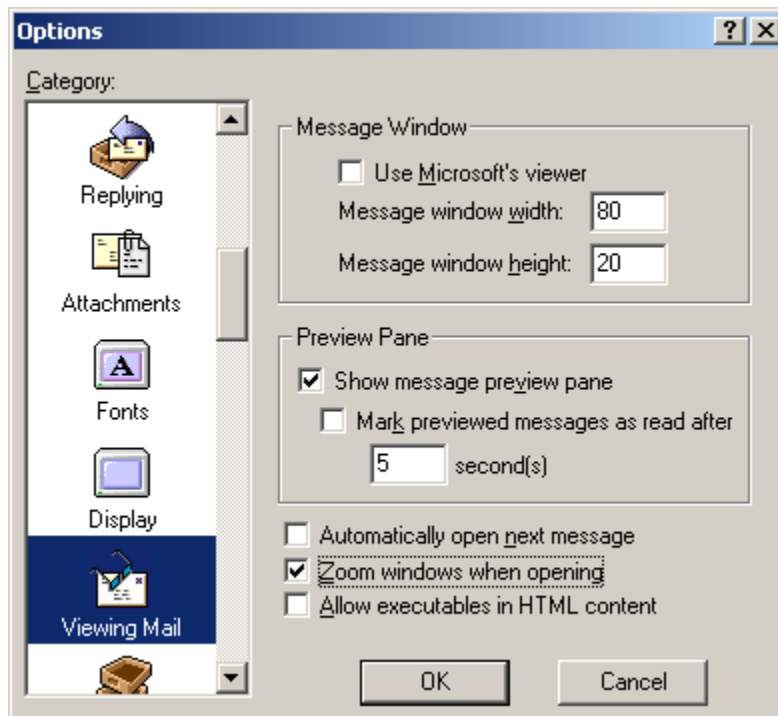
In this example, parent permissions are set to propagate to children elements, i.e. the **Eudora.ini** file. The message data files for this Eudora user are accessible by anyone with access to the machine. To prevent this from occurring during the installation process, install all Eudora data files into 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:

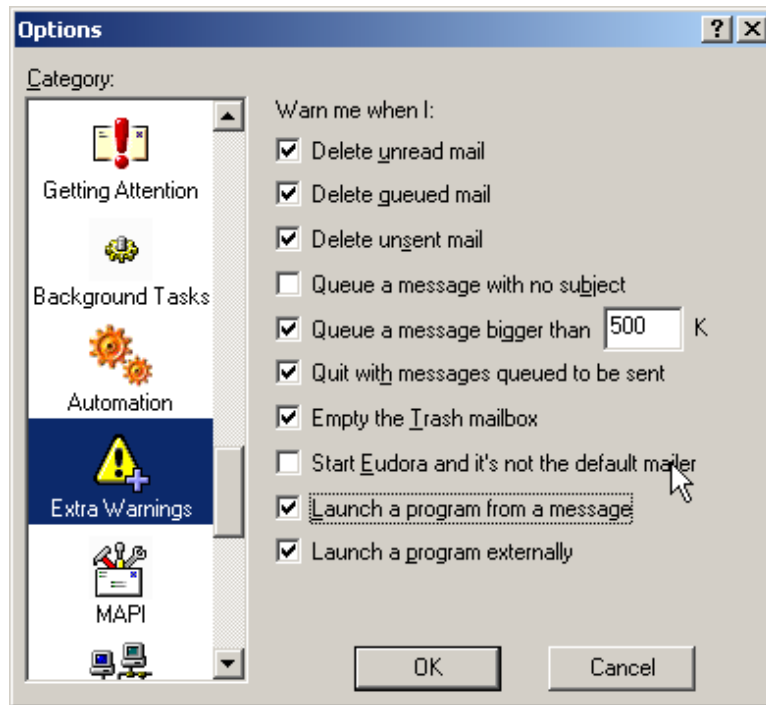
1. Start **Eudora**.
2. Edit Eudora options.
 - a. Click on the **Tools** menu option.
 - b. Click on the **Options** menu choice to open the Edit Options window.
3. Open Viewing Mail Option/Disallow Executables in HTML content

- 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 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 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 Internet Explorer

Internet Explorer 5.01 (IE) 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 operating system, 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 a certain actions. The possible levels of security are High, Medium, Medium-Low, and Low. Users can modify the security level for each of the Zones 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 Service Pack 2 provides 128 bits encryption as a default. It is recommended that Service Pack 2 be installed. If Service Pack 2 cannot be installed, the Windows 2000 Professional high encryption pack can be downloaded from the Windows Update site.

In general, 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. CERT and SANS 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 Internet Explorer:

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.

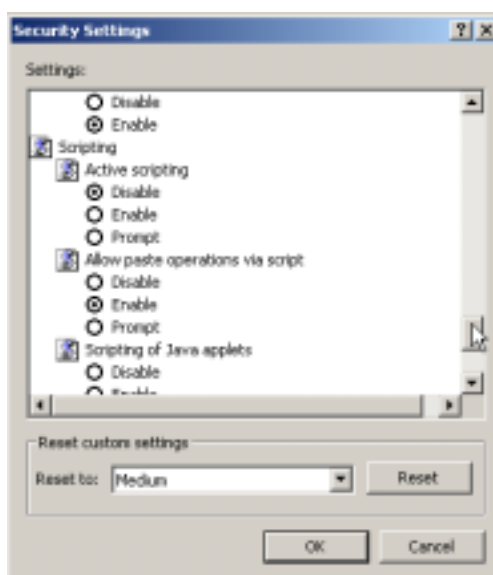
3. Scroll down to the setting labeled **Script ActiveX controls marked safe for scripting** in the **Security Settings** Dialog box and check the **Disable** option.

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.

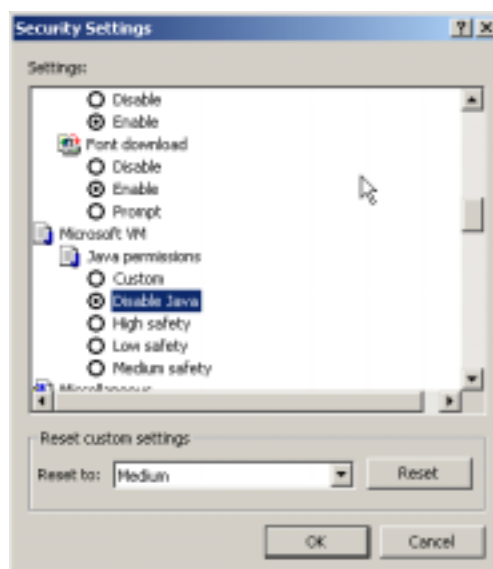
Figure 10-20: Disable Scripting in Internet Explorer



It is recommended to enable Java 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.

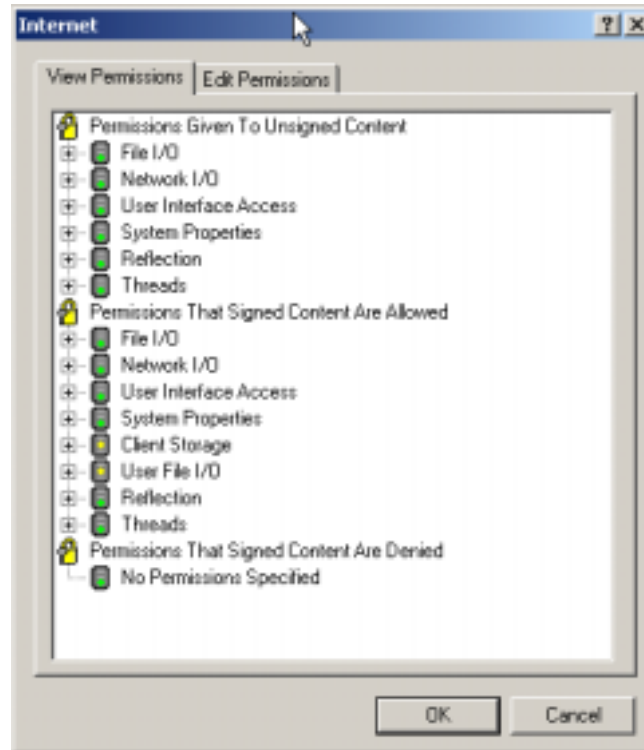
Figure 10-21: Disable Java in Internet Explorer



Note: Internet Explorer allows customizations of Java virtual machine (JVM) permissions by clicking on the **Custom** radio button under the **Java Permissions**. This 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

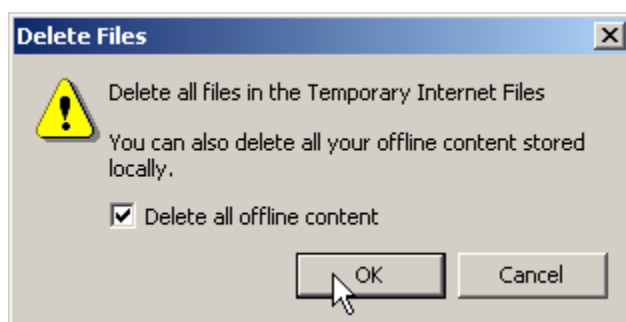


In terms of user privacy, the cache files collected by IE should be emptied after every Web session, unless the environment warrants their usage. A low-bandwidth Internet connection may provide value in the use of the cache for performance reasons yet in most other cases a user should take steps to ensure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

To empty the cache for Internet Explorer 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-sized 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. The following figure 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

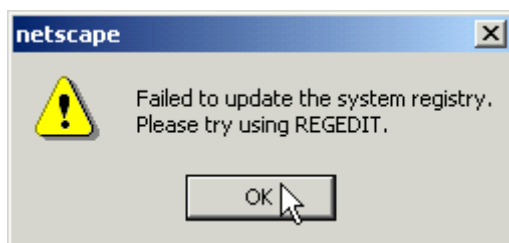


Table 10-1 lists the registry keys that Netscape attempts to unsuccessfully access when running the installation process as a regular user.

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. There are two methods for updating/upgrading Netscape:

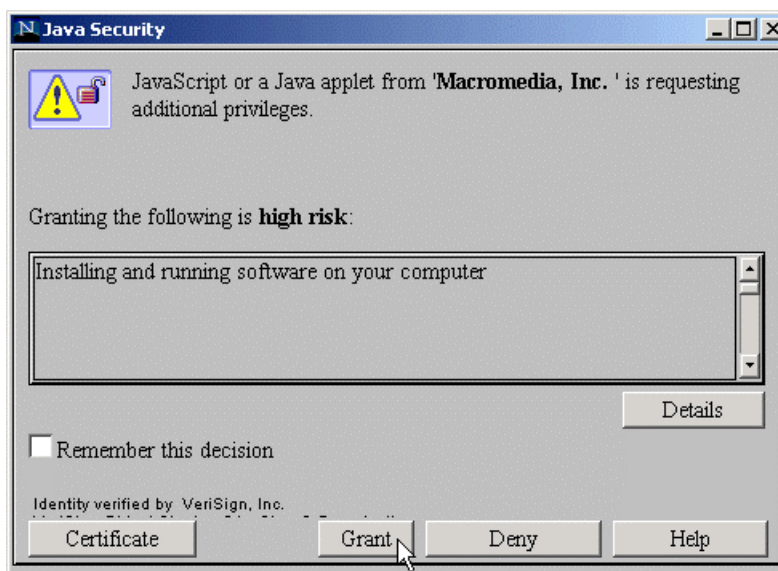
- Visiting the URLs noted above, these Web pages will automatically determine which version of Netscape is installed, and if a new version is available.
- Using SmartUpdate manager will determine if any updates are available.

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, which includes:

- 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 below shows. This dialog box recognizes a digitally signed Java applet. Netscape forces developers to sign applets based on permissions. Users are permitted to permit/deny any action they choose.

Figure 10-25: Netscape Communicator Update Requesting Java Permission



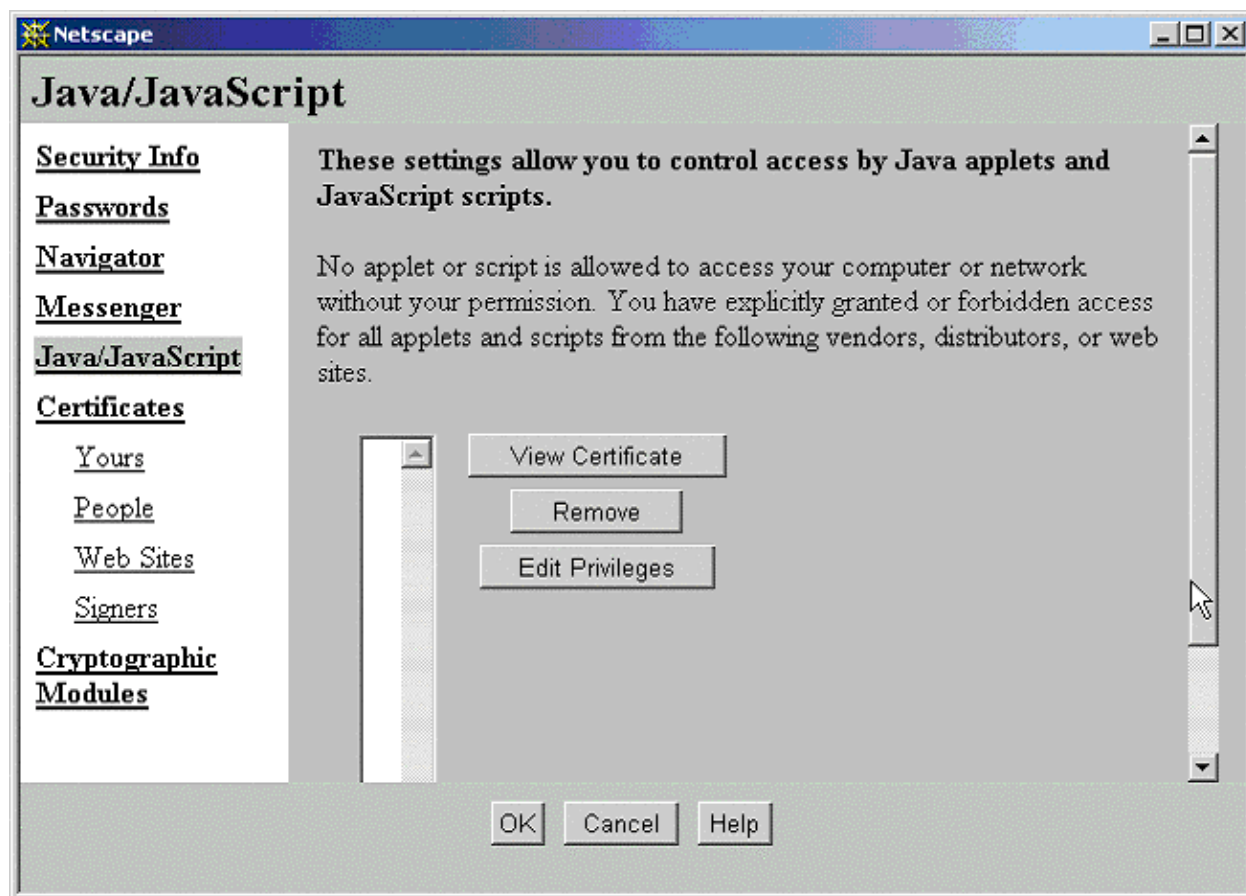
Users should not grant this software the permission to install unless they can be sure of the integrity of what they are installing. To prevent software from installing, press the **Deny** button shown in Figure 10-25.

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**.

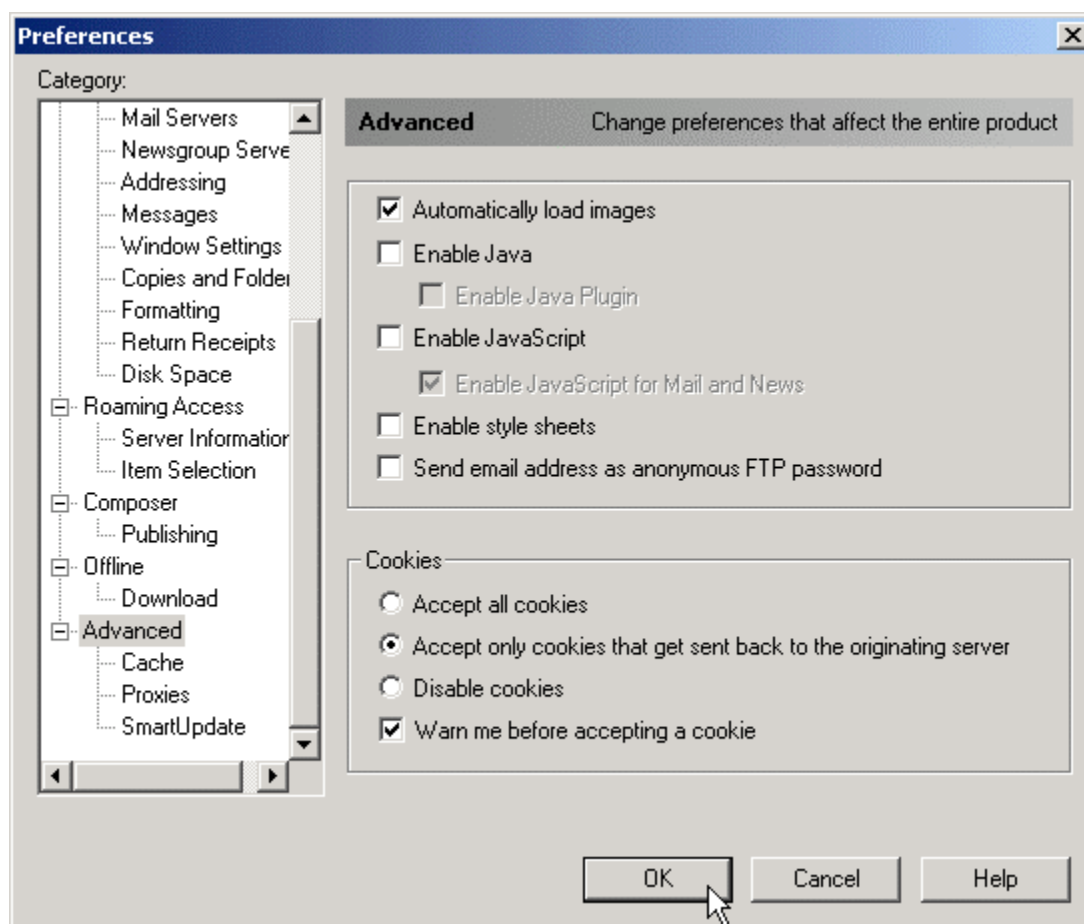
This file is stored in the **%SystemRoot%** folder by default. Default directory permissions prevent Netscape from modifying this file after installation. To enable Netscape to modify this file, it must allow the **Everyone** group read/write permission within its ACL.

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 Administrator or unless they are aware of the ramifications. As an example, users are prevented from updating Netscape with Active Content disabled.

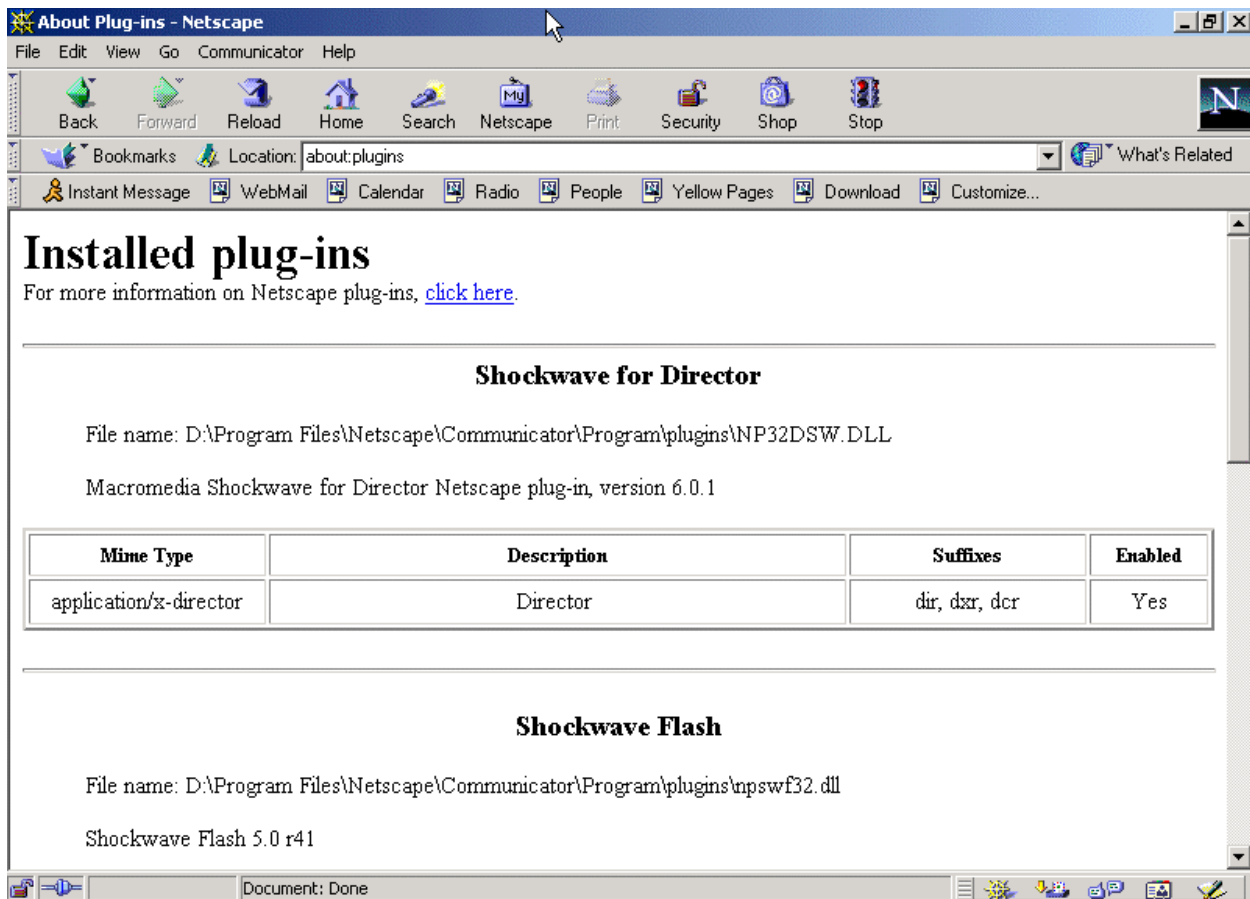
Figure 10-27: Disable Active Content within Netscape Communicator

Netscape differs from Internet Explorer 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 plug-in. To list what plug-ins Netscape currently has installed, select the **About Plug-ins** 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 below. This page, rendered by Netscape, lists information on all of the plug-ins currently installed.

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

Figure 10-28: Installed Netscape Plugins

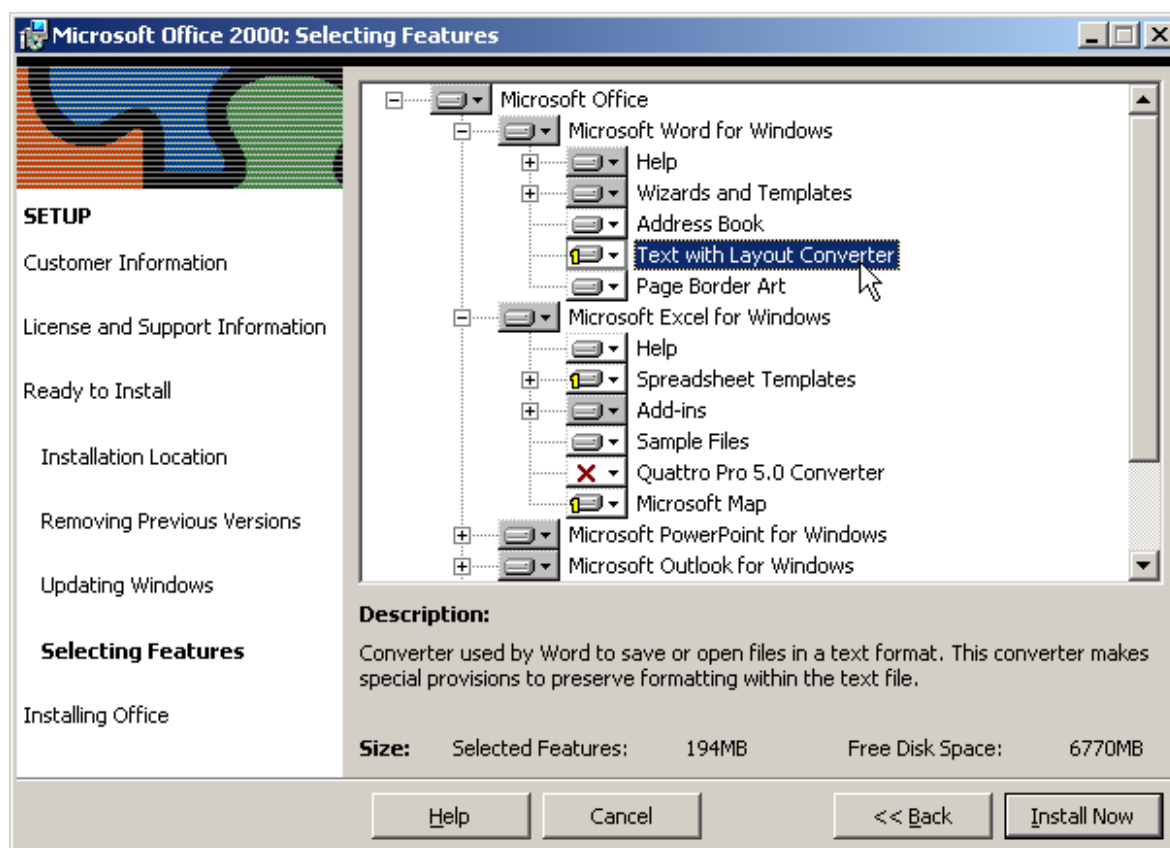
10.4 PRODUCTIVITY APPLICATIONS

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). VBA makes it simple to include an Excel spreadsheet in a Word document or vice versa. These applications also 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 both 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: Administrator 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 7.2.2, 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. While Office XP is commercially available, the current SR for Microsoft Office 2000 is SR-1.

Note: When deciding to install an SR, remember that they tend to be very large. Download and install the service pack 2, SP-2 and other post SP-2 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 where the Macro they are using came from. Office

2000 silently disables non-signed 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 helps reduce the spread of macro viruses. If all legitimate macros are digitally signed, then 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 Microsoft Visual Basic for Applications (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 only allows 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 allows users the opportunity to inspect the digital certificate, and 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

- Anti-Virus Scanners
 - Do not install competing Anti-Virus software on the same machine.
 - Ensure that Anti-Virus 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 Email and Internet scanning.
- Email 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.
 - 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 Browsers

NIST WIN2K DRAFT FOR PUBLIC COMMENT

- 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.

11. REMOTE SYSTEM SEAT MANAGEMENT

Windows 2000 Active Directory includes many built-in features for rapid deployment of Software, Service Packs, Operating Systems, and Patches. Using the Windows 2000 built-in features is the preferred method of software update and deployment in small to medium sized 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

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 operating system 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 organizational units (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 users 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) Dynamic Host Configuration (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 pre-configured 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 users 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 include SMS 2.0 and LanDesk 6.0. The additional security management features provided by these software packages will be mentioned 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 operating system 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 Administrator, 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 OS's, 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. SUMMARY

This guide is intended as administration guidance for the Window 2000 Professional operating system. The guide is based upon the recommendations of the NSA Windows 2000 Security guides and other documents produced by the security professional community. This guide attempts to present an overview of security practices and configurations to consider as well as recommended settings to implement when installing and supporting the Windows 2000 Professional operating system and selected applications. All of the recommendations presented herein have been tested on Windows 2000 Professional platforms both mobile and desktop. Be sure to follow instructions exactly as printed as deviations can have adverse and unpredictable effects. 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.

APPENDIX A: REGISTRY DISCUSSION

This section will present 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 programming APIs that Microsoft, and third party organizations have developed, there are numerous ways to access the registry both 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 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. Due to the fact that registry could conceivably grow very large in size, and the fact that it must 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 four levels, in a descending hierarchy:

- Hive keys – these keys are system defined prefixed with the letters **HKEY_**, and act as organizational assistants. Microsoft divides any sub-keys based upon purpose. The five hive keys are:

Hive Keys

HKEY_LOCAL_MACHINE (HKLM) – This hive contains operating system and hardware-oriented information. HKLM holds most of the information of the registry since two of the other four hive keys are aliased to its sub-keys.

HKEY_CURRENT_USER (HKCU) – This hive contains the user profile for the specific user that is currently logged into the system.

HKEY_CLASSES_ROOT (HKCR) – This hive contains sub-keys listing all of the COM servers currently registered on the computer and all file extensions currently associated with applications.

HKEY_USERS (HKU) – This hive contains sub-keys that contain all the user profiles for the current computer.
--

HKEY_CURRENT_CONFIG (HKCC) – This hive contains sub-keys 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 – Sub-keys are yet another level of organization for subsequent values and having 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. The following table lists the recognized data types for the Windows 2000 registry.

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	Multi-string	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

The most important point to make regarding the registry is 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 stressed 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 included 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 capabilities such as:

- Adding new registry keys
- Updating information in existing registry keys
- Removing registry keys
- Save registry keys to hive files
- Find specific registry keys or values

A discussion of security of the Windows 2000 Professional registry should include a discussion 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. There too many keys and values within the registry that store data that is of a sensitive nature to users of the system than can be mentioned in one discussion. It is important to know the default restrictions on the registry hives, because this leads a user into the determination of a plan of action should they be required to change the ACL settings later. The following table lists the default registry ACL information for Windows 2000 Professional.

The following conventions help to explain the information provided in the table below.

- SW stands for Software
- MS stands for Microsoft
- W stands for Windows
- W NT stands for Windows NT
- CV stands for Current Version

Default Registry ACLs

Registry Key/Hive	Default Power User Permissions	Default User Permissions
HKEY_LOCAL_MACHINE		
HKLM\Software	Modify	Read
HKLM\SW\Classes\helpfile	Read	Read
HKLM\SW\Classes\.hlp	Read	Read
HKLM\SW\MS\Command Processor	Read	Read
HKLM\SW\MS\Cryptography	Read	Read
HKLM\SW\MS\Driver Signing	Read	Read

Registry Key/Hive	Default Power User Permissions	Default User Permissions
HKLM\SW\MS\EnterpriseCertificates	Read	Read
HKLM\SW\MS\Non-Driver Signing	Read	Read
HKLM\SW\MS\NetDDE	None	None
HKLM\SW\MS\Ole	Read	Read
HKLM\SW\MS\Rpc	Read	Read
HKLM\SW\MS\Secure	Read	Read
HKLM\SW\MS\SystemCertificates	Read	Read
HKLM\SW\MS\Windows\CV\RunOnce	Read	Read
HKLM\SW\MS\W NT\CV\DiskQuota	Read	Read
HKLM\SW\MS\W NT\CV\Drivers32	Read	Read
HKLM\SW\MS\W NT\CV\Font Drivers	Read	Read
HKLM\SW\MS\W NT\CV\FontMapper	Read	Read
HKLM\SW\MS\W NT\CV\Image File Execution Options	Read	Read
HKLM\SW\MS\W NT\CV\IniFileMapping	Read	Read
HKLM\SW\MS\W NT\CV\Perflib	Read (via Interactive)	Read (via Interactive)
HKLM\SW\MS\W NT\CV\SecEdit	Read	Read
HKLM\SW\MS\W NT\CV\Time Zones	Read	Read
HKLM\SW\MS\W NT\CV\Windows	Read	Read
HKLM\SW\MS\W NT\CV\AsrCommands	Read	Read
HKLM\SW\MS\W NT\CV\Winlogon	Read	Read
HKLM\SW\MS\W NT\CV\Classes	Read	Read
HKLM\SW\MS\W NT\CV\Console	Read	Read

Registry Key/Hive	Default Power User Permissions	Default User Permissions
HKLM\SW\MS\W NT\CV\ProfileList	Read	Read
HKLM\SW\MS\W NT\CV\Svchost	Read	Read
HKLM\SW\Policies	Read	Read
HKLM\System	Read	Read
HKLM\SYSTEM\CCS\Control\SecurePipe Servers\winreg	None	None
HKLM\SYSTEM\CCS\Control\Session Manager\Executive	Modify	Read
HKLM\SYSTEM\CCS\Control\TimeZoneInformation	Modify	Read
HKLM\SYSTEM\CCS\Control\WMI\Security	None	None
HKLM\Hardware	Read (via Everyone)	Read (via Everyone)
HKLM\SAM	Read (via Everyone)	Read (via Everyone)
HKLM\Security	None	None
HKEY_USERS		
USERS\DEFAULT	Read	Read
USERS\DEFAULT\SW\MS\NetDDE	None	None
HKEY_CURRENT_CONFIG	= HKLM\System\CCS\HardwareProfiles\Current	
HKEY_CURRENT_USER	Full Control	Full Control
HKEY_CLASSES_ROOT	= HKLM\SW\Classes	

Note: Do not change any Access Control Entry on a registry hive without fully being 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. The following table describes the Windows 2000 Professional registry keys in detail.

Keys Modified by NIST template

Description and Data Type of Registry Keys		
Registry Value	HKEY_LOCAL_MACHINE\SOFTWARE\Windows NT\CurrentVersion\Winlogon\SFCSHOWProgress	
This registry setting hides the Windows File Protection progress display window from the user.		REG_DWORD
Registry Value :	HKEY_LOCAL_MACHINE\Software\microsoft\driver signing\policy	
This setting configures Windows 2000 to display a warning when it encounters a driver that has not been signed or signed incorrectly.		REG_BINARY
Registry Value :	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DrWatson\CreateCrashDump	
This setting 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 debugging purposes should be promptly deleted.		REG_DWORD
Registry Value :	HKEY_LOCAL_MACHINE\software\microsoft\non-driver signing\policy	
This setting configures Windows 2000 to display an alert when it encounters a piece of hardware without a digital signature.		REG_BINARY
Registry	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows	

Description and Data Type of Registry Keys		
Value :	NT\CurrentVersion\WinlogonDontDisplayLastUserName	
Enabling this key will blank the username box on the logon screen. Preventing people that 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	
This setting disables the Dr. Watson program debugger on Windows 2000 Professional. To re-enable the debugger type the following at the command line: C:\>drwtsn -l		REG_DWORD
Registry Value :	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SFCDisable	
This option 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	
This option configures the System File Checker to scan the protected files at every boot. This is resource intensive but there is a direct trade off with security, Implement a key like this only after serious consideration.		REG_DWORD
Registry Value :	HKEY_LOCAL_MACHINE\Software\Microsoft\windows nt\currentversion\winlogon\allocatcdroms	
Determines whether data in the CD-ROM 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 of 0 indicates that Compact discs in the CD-ROM drive can be accessed by all administrators in the domain. A value of 1		REG_SZ

Description and Data Type of Registry Keys	
means that only the user logged on locally can access data on the compact discs in the CD-ROM drive.	

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

Registry Value :	HKEY_LOCAL_MACHINE\Software\Microsoft\windows nt\currentversion\winlogon\allocatefloppies
<p>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.</p> <p>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.</p>	REG_SZ

Registry Value :	HKEY_LOCAL_MACHINE\Software\Microsoft\windows nt\currentversion\winlogon\cachedlogonscount
This setting determines the number of previous logons that the operating system will cache in the event that a domain controller cannot be contacted. When set to 0 users will not be able to logon to their domain account unless a domain controller is available.	REG_DWORD

Registry Value :	HKEY_LOCAL_MACHINE\Software\Microsoft\windows nt\currentversion\winlogon\passwordexpirywarning
This setting displays a warning to the user when their password is about to expire. The amount of time before this warning is given can be set in the value.	REG_BINARY

Registry	HKEY_LOCAL_MACHINE\Software\Microsoft\windows
----------	---

Description and Data Type of Registry Keys		
Value :	nt\currentversion\winlogon\scremoveoption	
Controls if users can remove smart cards from readers. Removing smart cards has been shown to cause applications that use smart cards to behave insecurely and as such users should be prevented from doing so.		REG_DWORD

Registry Value :	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AutoAdminLogon	
This setting has the ability to bypass the logon prompt. It 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 due to the security implications of its misuse.		REG_SZ

Registry Value :	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\NetworkHideSharePwds	
This setting controls whether the password typed when accessing a file share is shown in clear text or as asterisks. This 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	
It's possible for users to setup a modem on a Windows machine, and by using Dial-up Networking allow callers to connect to the internal network. Especially in a corporate environment this can cause a major security risk. Exit your registry, you may need to restart or log out of Windows for the change to take effect.		REG_DWORD

Registry Value :	HKEY_LOCAL_MACHINE\Software\Microsoft\windows\currentversion\policies\System\disablecad	
This setting determines whether users must press the Ctrl+Alt+Del security attention sequence to log on to Windows 2000. Enabling this setting is not recommended since the secure attention sequence has the ability to bypass Trojan logon prompts. Never		REG_DWORD

Description and Data Type of Registry Keys	
log into a computer that displays the logon prompt automatically, always press Ctrl+Alt+Del to display it.	

Registry Value :	HKEY_LOCAL_MACHINE\Software\Microsoft\windows\currentversion\policies\System\dontdisplaylastusername
This setting prevents the logon screen from displaying the last know user that 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
This setting 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\Explorer\NoDriveTypeAutoRun
This setting disables the auto-run 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 auto run enabled.	REG_DWORD

Registry Value :	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl\AutoReboot
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

Description and Data Type of Registry Keys

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. You can disable this discovery by preventing anonymous connections to domains using the following Windows NT registry hack. Caution: this can have severe consequences on SQL Server access and creating/maintaining domain trusts.	REG_DWORD

Registry Value :	HKEY_LOCAL_MACHINE\System\CurrentControlSet\control\session manager\memory management\clearpagefileatshutdown
This value specifies that the memory page file pagefile.sys will be cleared each time the machine is powered down preventing data reminisce. Since the pagefile is inaccessible during runtime, this is unnecessary to do while the computer is on.	REG_DWORD

Registry Value :	HKEY_LOCAL_MACHINE\System\CurrentControlSet\control\session manager\protectionmode
This setting adds strong protection over shared objects. It will prevent users from unauthorized access to the known 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	HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\lanmanse
----------	---

Description and Data Type of Registry Keys		
Value :	rver\parameters\enableforcedlogoff	
This setting enables the operating system to perform a forced logoff of a user that is logged into Windows 2000 Professional.		REG_DWORD

Registry Value :	HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\lanmanse rver\parameters\enablesecuritysignature	
This setting enables the operating system to digitally sign all network SMB traffic to servers.		REG_DWORD

Registry Value :	HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\lanmanwo rkstation\parameters\enablesecuritysignature	
This setting enables the operating system to digitally sign all network SMB traffic to clients.		REG_DWORD

Registry Value :	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MrxSm b\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	
This setting specifies the requirement of securing the communications, by encrypting or digitally signing, between a client and a domain controller.		REG_DWORD

Registry	HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\netlogon\	
----------	--	--

Description and Data Type of Registry Keys		
Value :	parameters\requirestrongkey	
This setting 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	
This setting requires encrypting the communications between a client and domain controller.		REG_DWORD

Registry Value :	HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\netlogon\parameters\signsecurechannel	
This setting 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\EnableICMPRedirects	
This parameter controls whether Windows 2000 will alter its route table in response to 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	
------------------	---	--

Description and Data Type of Registry Keys	
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 administrator 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 RCE (route cache entry) creation if the TcpMaxHalfOpen and	REG_DWORD

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

Registry Value :	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxHalfOpen
This key 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 listen backlog on the port you want to protect.	REG_DWORD

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

APPENDIX B: WINDOWS 2000 SECURITY TEMPLATES

This appendix discusses security templates for Windows 2000. This document provides sample security templates for use with Windows 2000 Professional, for both domain members and stand-alone machines. Due to the extremely large diversity of computing environments, exercise caution when applying these templates to an installation of Windows 2000 Professional.

Sample provided Windows 2000 security templates

Sample Windows 2000 Security Templates	
Template	Description
NIST2kws.inf	This template is designed for stand-alone installations of Windows 2000 Professional.
NIST2kdm.inf	This template is designed for Windows 2000 Professional domain members.

Users that examine these templates will find some settings disabled by default. While 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.

Template Security Settings

Listed below are the additional settings and descriptions included in the NIST .inf files. The Bolded text is the actual entries included in the .inf files.

B.1 Account Policies

This section defines parameters for account security and password policy. They correspond to the Account policies section of the Local Security policy MMC snap-in.

✓	Password Policy	Recommended Computer Setting
	Enforce password history	24 passwords remembered
	Maximum password age	90 days
	Minimum password age	1 days
	Minimum password length	8 characters
	Passwords must meet complexity requirements	Enabled
	Store password using reversible encryption for all users in the domain	Disabled

✓	Account Lockout Policy	Recommended Computer Setting
	Account lockout duration	15 minutes
	Account lockout threshold	3 invalid logon attempts
	Reset account lockout counter after	15 minutes

✓	Kerberos Policy	Recommended Computer Setting
	Enforce user logon restrictions	Not defined
	Maximum lifetime for service ticket	Not defined
	Maximum lifetime for user ticket	Not defined
	Maximum lifetime for user ticket renewal	Not defined
	Maximum tolerance for computer clock synchronization	Not defined

B.2 Local Policies

The Local Policies area of the Template defines the policies for the System Auditing Policy, User rights assignment, and Security Options. The following table defines the settings in the NIST template.

✓	Audit Policy	Recommended Computer Setting
	Audit account logon events	Success, Failure
	Audit account management	Success, Failure
	Audit directory service access	No auditing
	Audit logon events	Success, Failure
	Audit object access	Failure
	Audit policy change	Success, Failure
	Audit privilege use	Failure
	Audit process tracking	No auditing
	Audit system events	Success, Failure

✓	User Rights Assignment	Recommended Computer Setting
	Access this computer from the network	Users, Administrators
	Act as part of the operating system	
	Add workstations to domain	
	Back up files and directories	Administrators
	Bypass traverse checking	Users
	Change the system time	Administrators
	Create a pagefile	Administrators
	Create a token object	
	Create permanent shared objects	
	Debug programs	
	Deny access to this computer from the network	
	Deny logon as a batch job	
	Deny logon as a service	
	Deny logon locally	
	Enable computer and user accounts to be trusted for delegation	
	Force shutdown from a remote system	Administrators
	Generate security audits	
	Increase quotas	Administrators
	Increase scheduling priority	Administrators

NIST WIN2K DRAFT FOR PUBLIC COMMENT

✓	User Rights Assignment	Recommended Computer Setting
	Load and unload device drivers	Administrators
	Lock pages in memory	
	Log on as a batch job	
	Log on as a service	
	Log on locally	Users, Administrators
	Manage auditing and security log	Administrators
	Modify firmware environment values	Administrators
	Profile single process	Administrators
	Profile system performance	Administrators
	Remove computer from docking station	Users, Administrators
	Replace a process level token	
	Restore files and directories	Administrators
	Shut down the system	Users, Administrators
	Synchronize directory service data	
	Take ownership of files or other objects	Administrators

✓	Security Options	Recommended Computer 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	Not defined
	Automatically log off users when logon time expires (local)	Enabled
	Clear virtual memory pagefile when system shuts down	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	Insert recommended logon banner for your environment here.
	Message title for users attempting to log on	Insert title of the logon banner window here.
	Number of previous logons to cache (in case domain controller is not available)	0 logons
	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 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	Disabled

✓	Security Options	Recommended Computer Setting
	(always)	
	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
	Secure system partition (for RISC platforms only)	Not defined
	Send unencrypted password to connect to third-party SMB servers	Disabled
	Shut down system immediately if unable to log security audits	Disabled (Enable this setting in high security risk environment)
	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 non-driver installation behavior	Warn but allow installation

B.3 Event Log Settings

For the log settings below, the default maximum size is 4GB 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. You should 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.

✓	Event Log Policy	Recommended Computer Setting
	Maximum application log size	4194240 kilobytes
	Maximum security log size	4194240 kilobytes
	Maximum system log size	4194240 kilobytes
	Restrict guest access to application log	Enabled
	Restrict guest access to security log	Enabled
	Restrict guest access to system log	Enabled
	Retain application log	7 days
	Retain security log	7 days
	Retain system log	7 days
	Retention method for application log	Manually
	Retention method for security log	Manually
	Retention method for system log	Manually
	Shut down the computer when the security audit log is full	Disabled

B.4 Restricted Groups

The Restricted Groups Policy area of the Template is for administration of local groups the recommended settings for the NIST template is shown in the Table below.

✓	Group Name	Members	Member Of
	Power Users		

B.5 System Services

The recommended method of starting various System Services is defined in the table below.

Permissions Key:
 Full Control = FC
 Read = R
 Start, Stop and Pause = SSP
 Write = W
 Delete = Del

✓	Service Name	Startup	Permission
	Alerter	Not Defined in the template, refer to Table 8-1 for recommendation.	Not defined
	Application Management	Manual	Administrators – FC
	ClipBook	Manual	Administrators - FC
	COM+ Event System	Disabling this service may cause system instability	Not defined
	Computer Browser	Automatic	Administrators – FC Authenticated Users – R Power Users – R SYSTEM – R,SSP
	DHCP Client	Not Defined in the template, refer to Table 8-1 for recommendation.	Administrators – FC Authenticated Users – R Power Users – R SYSTEM – R,SSP
	Distributed Link Tracking Client	Not Defined in the template, refer to Table 8-1 for recommendation.	Administrators – FC Authenticated Users – R Power Users – R SYSTEM – R,SSP
	Distributed Transaction Coordinator	Disabling this service may cause system instability	Not defined
	DNS Client	Automatic	Administrators – FC Authenticated Users – R Power Users – R SYSTEM – R,SSP
	Event Log	Automatic	Administrators – FC Authenticated Users – R Power Users – R SYSTEM – R,SSP
	Fax Service	Not Defined in the template, refer to Table 8-1 for recommendation.	Not defined
	Indexing Service	Not Defined in the template, refer to Table 8-1 for recommendation.	Not defined
	Infrared Monitor	Not Defined in the template, refer to Table 8-1 for recommendation.	Not defined
	Internet Connection Sharing	Disabled	Administrators - FC
	IPSEC Policy Agent	Automatic	Administrators – FC Power Users – R SYSTEM – R,SSP
	Logical Disk Manager	Automatic	Administrators – FC Authenticated Users – R

NIST WIN2K DRAFT FOR PUBLIC COMMENT

✓	Service Name	Startup	Permission
			Power Users – R SYSTEM – R,SSP
	Logical Disk Manager Administrative Service	Not defined	Not defined
	Messenger	Not Defined in the template, refer to Table 8-1 for recommendation.	Administrators – FC Authenticated Users – R Power Users – R SYSTEM – R,SSP
	Net Logon	Not defined	Not defined
	NetMeeting Remote Desktop Sharing	Not Defined in the template, refer to Table 8-1 for recommendation.	Not defined
	Network Connections	Disabling this service may cause system instability	Not defined
	Network DDE	Manual	Administrators - FC
	Network DDE DSDM	Manual	Administrators - FC
	NT LM Security Support Provider	Disabling this service may cause system instability	Not defined
	Performance Logs and Alerts	Not Defined in the template, refer to Table 8-1 for recommendation.	Not defined
	Plug and Play	Automatic	Administrators – FC Authenticated Users – R Power Users – R SYSTEM – R,SSP
	Print Spooler	Automatic	Administrators – FC Authenticated Users – R Power Users – R SYSTEM – R,SSP
	Protected Storage	Automatic	Administrators – FC Authenticated Users – R Power Users – R SYSTEM – R,SSP
	QoS RSVP	Disabling this service may cause system instability	Not defined
	Remote Access Auto Connection Manager	Not Defined in the template, refer to Table 8-1 for recommendation.	Not defined
	Remote Access Connection Manager	Not Defined in the template, refer to Table 8-1 for recommendation.	Not defined
	Remote Procedure Call (RPC)	Automatic	Administrators - FC
	Remote Procedure Call (RPC) Locator	Not Defined in the template, refer to Table 8-1 for recommendation.	Not defined
	Remote Registry Service	Not Defined in the template, refer to Table 8-1 for recommendation.	Administrators – FC Authenticated Users – R Power Users – R SYSTEM – R,SSP
	Removable Storage	Automatic	Administrators – FC Authenticated Users – R Power Users – R SYSTEM – R,SSP
	Routing and Remote Access	Disabled	Administrators – FC
	RunAs Service	Not Defined in the template, refer to Table 8-1 for	Administrators – FC Authenticated Users – R

✓	Service Name	Startup	Permission
		recommendation.	Power Users – R SYSTEM – R,SSP
	Security Accounts Manager	Automatic	Administrators – FC
	Server	Not Defined in the template, refer to Table 8-1 for recommendation.	Administrators – FC Authenticated Users – R Power Users – R SYSTEM – R,SSP
	Smart Card	Not Defined in the template, refer to Table 8-1 for recommendation.	Not defined
	Smart Card Helper	Not Defined in the template, refer to Table 8-1 for recommendation.	Not defined
	System Event Notification	Automatic	Administrators – FC Authenticated Users – R Power Users – R SYSTEM – R,SSP
	Task Scheduler	Disabled	Administrators – FC SYSTEM – R,SSP
	TCP/IP NetBIOS Helper Service	Automatic	Administrators – FC Authenticated Users – R Power Users – R SYSTEM – R,SSP
	Telephony	Disabling this service may cause system instability	Not defined
	Telnet	Disabled	Administrators - FC
	Uninterruptible Power Supply	Not Defined in the template, refer to Table 8-1 for recommendation.	Not defined
	Utility Manager	Not Defined in the template, refer to Table 8-1 for recommendation.	Not defined
	Windows Installer	Disabling this service may cause system instability	Not defined
	Windows Management Instrumentation	Not Defined in the template, refer to Table 8-1 for recommendation.	Not defined
	Windows Management Instrumentation Driver Extensions	Not Defined in the template, refer to Table 8-1 for recommendation.	Not defined
	Windows Time	Not Defined in the template, refer to Table 8-1 for recommendation.	Not defined
	Workstation	Automatic	Administrators – FC Authenticated Users – R Power Users – R SYSTEM – R,SSP

B.6 Registry Modifications

The table below lists the registry modifications made by the NIST template.

✓	Registry Value :	Data Type	Recommended Value
	HKEY_LOCAL_MACHINE\SOFTWARE\Windows NT\CurrentVersion\Winlogon\SFCSHOWProgress	REG_DWORD	0
	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\ExplorerNoLogOff	REG_BINARY	01 00 00 00
	HKEY_LOCAL_MACHINE\Software\microsoft\driver signing\policy	REG_BINARY	01
	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DrWatson\CreateCrashDump	REG_DWORD	0
	HKEY_LOCAL_MACHINE\software\microsoft\non-driver signing\policy	REG_BINARY	01
	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\WinlogonDontDisplayLastUserName	REG_SZ	1
	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug\Auto	REG_DWORD	0
	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SFCDisable	REG_DWORD	4
	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SFCSan	REG_DWORD	1
	HKEY_LOCAL_MACHINE\Software\Microsoft\windows nt\currentversion\winlogon\allocateddrams	REG_SZ	1
	HKEY_LOCAL_MACHINE\Software\Microsoft\windows nt\currentversion\winlogon\allocatedasd	REG_SZ	0
	HKEY_LOCAL_MACHINE\Software\Microsoft\windows nt\currentversion\winlogon\allocatefloppies	REG_SZ	1
	HKEY_LOCAL_MACHINE\Software\Microsoft\windows nt\currentversion\winlogon\cachedlogonscount	REG_DWORD	1
	HKEY_LOCAL_MACHINE\Software\Microsoft\windows nt\currentversion\winlogon\passwordexpirywarning	REG_BINARY	14
	HKEY_LOCAL_MACHINE\Software\Microsoft\windows nt\currentversion\winlogon\scremoveoption	REG_DWORD	0

✓	Registry Value :	Data Type	Recommended Value
	ows nt\currentversion\winlogon\scremoveoption		
	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AutoAdminLogon	REG_SZ	0
	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\NetworkHideSharePwds	REG_DWORD	1
	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\NetworkNoDialIn	REG_DWORD	1
	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\currentversion\policies\System\disablecad	REG_DWORD	0
	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\currentversion\policies\System\dontdisplaylastuserame	REG_DWORD	1
	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\currentversion\policies\System\shutdownwithoutlogon	REG_DWORD	0
	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun	REG_DWORD	0
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControlAutoReboot	REG_DWORD	0
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\RestrictAnonymous	REG_DWORD	2
	HKEY_LOCAL_MACHINE\System\CurrentControlSet\control\session manager\memory management\clearpagefileatshutdown	REG_DWORD	1
	HKEY_LOCAL_MACHINE\System\CurrentControlSet\control\session manager\protectionmode	REG_DWORD	1
	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\ParametersAutoShareWks	REG_DWORD	0
	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters\enableforcedl	REG_DWORD	1

✓	Registry Value :	Data Type	Recommended Value
	ogoff		
	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\lanmanserver\parameters\enablesecuritysignature	REG_DWORD	1
	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\lanmanworkstation\parameters\enablesecuritysignature	REG_DWORD	1
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MrxSmb\ParametersRefuseReset	REG_DWORD	1
	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\netlogon\parameters\requiresignorseal	REG_DWORD	0
	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\netlogon\parameters\requirestrongkey	REG_DWORD	0
	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\netlogon\parameters\sealsecurechannel	REG_DWORD	1
	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\netlogon\parameters\signsecurechannel	REG_DWORD	1
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableDeadGWDetect	REG_DWORD	0
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirects	REG_DWORD	0
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnablePMTUDiscovery	REG_DWORD	1
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTime	REG_DWORD	300000
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\NoNameReleaseOnDemand	REG_DWORD	1
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\PerformRouterDisc	REG_DWORD	0

✓	Registry Value :	Data Type	Recommended Value
	overy		
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect	REG_DWORD	2
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxHalfOpen	REG_DWORD	100
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxHalfOpenRetried	REG_DWORD	80

B.7 File Permissions

This section 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

%SystemDirectory% = C:\winnt\system32

%systemroot% = C:\winnt

%systemdrive% = C:

Permissions Key

Full Control = FC

Modify = M

Read and Execute = RX

List Folder Contents = L

Read = R

Write = W

✓	File Object Name	Permission
	%ProgramFiles%	Replace with Administrators = FC CREATOR OWNER = SYSTEM = FC USERS = RX,L,R
	%SystemDirectory%	Replace with Administrators = FC CREATOR OWNER = SYSTEM = FC USERS = RX,L,R
	%SystemDirectory%\appmgmt.dll	Replace with Administrator = FC SYSTEM = FC
	%SystemDirectory%\config	Replace with Administrators = FC SYSTEM = FC
	%SystemDirectory%\dllcache	Replace with Administrators = FC CREATOR OWNER = FC

NIST WIN2K DRAFT FOR PUBLIC COMMENT

✓	File Object Name	Permission
		SYSTEM = FC
	%SystemDirectory%\DTCLog	Replace with Administrators = FC CREATOR OWNER = FC USERS = RX SYSTEM = FC
	%SystemDirectory%\GroupPolicy	Replace with Administrators = FC Authenticated Users = RX, L, R SYSTEM = FC
	%SystemDirectory%\ias	Replace with Administrators = FC CREATOR OWNER = FC SYSTEM = FC
	%SystemDirectory%\Ntbackup.exe	Replace with Administrators = FC SYSTEM = FC
	%SystemDirectory%\NTMSData	Replace with SYSTEM = FC
	%SystemDirectory%\rcp.exe	Replace with Administrators = FC SYSTEM = FC
	%SystemDirectory%\rexec.exe	Replace with Administrators = FC SYSTEM = FC
	%SystemDirectory%\rsh.exe	Replace with Administrators = FC SYSTEM = FC
	%SystemDirectory%\secedit.exe	Replace with Administrators = FC SYSTEM = FC
	%SystemDirectory%\Setup	Replace with Administrators = FC USERS = RX,L,R SYSTEM = FC
	%SystemDirectory%\spool\printers	Replace with Administrators = FC CREATOR OWNER = FC SYSTEM = FC USERS = Special
	%SystemDrive%\autoexec.bat	Replace with Administrators = FC SYSTEM = FC USERS = RX,L,R
	%SystemDrive%\boot.ini	Replace with Administrators = FC SYSTEM = FC
	%SystemDrive%\config.sys	Replace with Administrators = FC SYSTEM = FC USERS = RX,L,R
	%SystemDrive%\Documents and Settings	Replace with Administrators = FC SYSTEM = FC USERS = RX,L,R

NIST WIN2K DRAFT FOR PUBLIC COMMENT

✓	File Object Name	Permission
	%SystemDrive%\Documents and Settings\Administrator	Replace with Administrators = FC SYSTEM = FC
	%SystemDrive%\Documents and Settings\All Users	Replace with Administrators = FC SYSTEM = FC USERS = RX,L,R
	%SystemDrive%\Documents and Settings\All Users\Documents\DrWatson	Replace with Administrator = FC CREATOR OWNER = FC SYSTEM = FC USERS = RX,L,R
	%SystemDrive%\Documents and Settings\All Users\Documents\DrWatson\drwtsn32.log	Replace with Administrator = FC CREATOR OWNER = FC SYSTEM = FC USERS = M
	%SystemDrive%\Documents and Settings\Default User	Replace with Administrator = FC SYSTEM = FC USERS = RX,L,R
	%SystemDrive%\IO.SYS	Replace with Administrator = FC SYSTEM = FC USERS = RX,L,R
	%SystemDrive%\MSDOS.SYS	Replace with Administrator = FC SYSTEM = FC USERS = RX,L,R
	%SystemDrive%\ntdetect.com	Replace with Administrator = FC SYSTEM = FC
	%SystemDrive%\ntldr	Replace with Administrator = FC SYSTEM = FC
	%SystemRoot%	Replace with Administrator = FC CREATOR OWNER = FC SYSTEM = FC USERS = RX
	%SystemRoot%\\$NtServicePackUninstall\$	Replace with Administrator = FC SYSTEM = FC
	%SystemRoot%\CSC	Replace with Administrator = FC SYSTEM = FC
	%SystemRoot%\regedit.exe	Replace with Administrator = FC SYSTEM = FC
	%SystemRoot%\repair	Replace with Administrator = FC SYSTEM = FC
	%SystemRoot%\security	Replace with Administrator = FC CREATOR OWNER = FC SYSTEM = FC
	%SystemRoot%\Temp	Replace with

NIST WIN2K DRAFT FOR PUBLIC COMMENT

✓	File Object Name	Permission
		Administrator = FC CREATOR OWNER = FC SYSTEM = FC USERS = RX,W
	c:\autoexec.bat	Replace with Administrator = FC SYSTEM = FC USERS = RX,L,R
	c:\boot.ini	Replace with Administrator = FC SYSTEM = FC
	c:\config.sys	Replace with Administrator = FC SYSTEM = FC USERS = RX
	c:\ntdetect.com	Replace with Administrator = FC SYSTEM = FC
	c:\ntldr	Replace with Administrator = FC SYSTEM = FC
	%SystemDirectory%\arp.exe	Replace with Administrator = FC SYSTEM = FC
	%SystemDirectory%\at.exe	Replace with Administrator = FC SYSTEM = FC
	%SystemDirectory%\cacls.exe	Replace with Administrator = FC SYSTEM = FC
	%SystemDirectory%\cmd.exe	Replace with Administrator = FC SYSTEM = FC
	%SystemDirectory%\cscript.exe	Replace with Administrator = FC SYSTEM = FC
	%SystemDirectory%\debug.exe	Replace with Administrator = FC SYSTEM = FC
	%SystemDirectory%\edit.com	Replace with Administrator = FC SYSTEM = FC
	%SystemDirectory%\edlin.exe	Replace with Administrator = FC SYSTEM = FC
	%SystemDirectory%\finger.exe	Replace with Administrator = FC SYSTEM = FC
	%SystemDirectory%\ftp.exe	Replace with Administrator = FC SYSTEM = FC
	%SystemDirectory%\ipconfig.exe	Replace with Administrator = FC SYSTEM = FC
	%SystemDirectory%\ipxroute.exe	Replace with Administrator = FC

NIST WIN2K DRAFT FOR PUBLIC COMMENT

✓	File Object Name	Permission
		SYSTEM = FC
	%SystemDirectory%\irftp.exe	Replace with Administrator = FC SYSTEM = FC
	%SystemDirectory%\nbtstat.exe	Replace with Administrator = FC SYSTEM = FC
	%SystemDirectory%\net.exe	Replace with Administrator = FC SYSTEM = FC
	%SystemDirectory%\netsh.exe	Replace with Administrator = FC SYSTEM = FC
	%SystemDirectory%\nslookup.exe	Replace with Administrator = FC SYSTEM = FC
	%SystemDirectory%\nwscript.exe	Replace with Administrator = FC SYSTEM = FC
	%SystemDirectory%\pathping.exe	Replace with Administrator = FC SYSTEM = FC
	%SystemDirectory%\ping.exe	Replace with Administrator = FC SYSTEM = FC
	%SystemDirectory%\regedt32.exe	Replace with Administrator = FC SYSTEM = FC
	%SystemDirectory%\regsvr32.exe	Replace with Administrator = FC SYSTEM = FC
	%SystemDirectory%\route.exe	Replace with Administrator = FC SYSTEM = FC
	%SystemDirectory%\runas.exe	Replace with Administrator = FC SYSTEM = FC
	%SystemDirectory%\runonce.exe	Replace with Administrator = FC SYSTEM = FC
	%SystemDirectory%\syskey.exe	Replace with Administrator = FC SYSTEM = FC
	%SystemDirectory%\telnet.exe	Replace with Administrator = FC SYSTEM = FC
	%SystemDirectory%\tftp.exe	Replace with Administrator = FC SYSTEM = FC
	%SystemDirectory%\tracert.exe	Replace with Administrator = FC SYSTEM = FC
	%SystemDirectory%\wscript.exe	Replace with Administrator = FC SYSTEM = FC
	%SystemDirectory%\xcopy.exe	Replace with

NIST WIN2K DRAFT FOR PUBLIC COMMENT

✓	File Object Name	Permission
		Administrator = FC SYSTEM = FC
	%SystemRoot%	Replace with Administrators =FC CREATOR OWNER = FC SYSTEM = FC Users = RX,L,R
	%SystemRoot%\debug	Replace with Administrators =FC CREATOR OWNER = FC SYSTEM = FC Users = RX,L,R
	%SystemRoot%\Registration	Replace with Administrators =FC SYSTEM = FC Users = R
	%SystemRoot%\tasks	Replace with Administrators =FC CREATOR OWNER = SYSTEM = FC Users = RX,L,R
	%SystemDrive%\	Replace with Administrators =FC CREATOR OWNER = SYSTEM = FC Users = RX,L,R
	%SystemRoot%\Debug\UserMode	Replace with Administrators =FC SYSTEM = FC Users = Special
	%SystemDrive%\ServicePackFiles	Replace with Administrators =FC SYSTEM = FC

APPENDIX C: TOOLS

This list provides a summary of the various tools that can be use 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
Caccls.exe	Command line interface used to display and modify ACLs of files.	Included with Windows 2000 systems
Hfnetchk.exe	Command line tool to allow Administrators 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 Administrators 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

NIST WIN2K DRAFT FOR PUBLIC COMMENT

MSPA	Microsoft Personal Security Advisor (MPSA), an ActiveX security control vulnerability scanner.	The MPSA generates a report of necessary fixes to address in order of criticality. It is found at: http://www.microsoft.com/technet/mpsa/start.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

APPENDIX D: WINDOWS XP SECURITY COMPONENTS OVERVIEW

This section 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 is provided for informational purposes only. The benefits listed within this section have neither been fully tested nor verified.

D.1 Windows XP Background

Windows XP, originally code-named Whistler, is sold in three distinct versions: one version 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

Windows XP (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 together 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 IEEE1394 networks. Bridging allows these two networks to act as a single network with a single 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 operating system. 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 automatically detects a move to a new access point, forcing re-authentication to ensure appropriate network access and detects 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.

D.4 Remote Assistance

Default Remote Assistance features are a new addition to XP. Remote Assistance offers services similar to those provided by software titles such as 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.

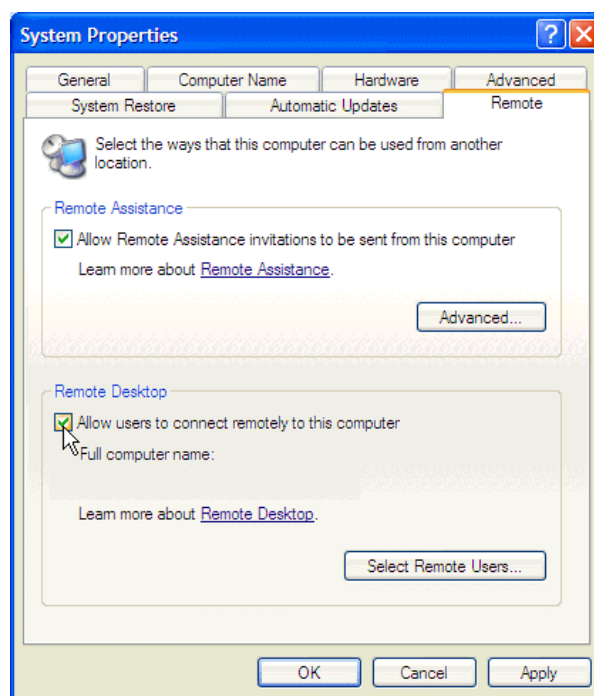
D.5 Remote Desktop Services

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 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 you to run an audio-enabled application on your remote desktop and hear the audio output from speakers attached to the computer you're working on.
- **Clipboard.** The Remote Desktop and the client computer share a clipboard that allows data to be interchanged.

XP Remote Desktop

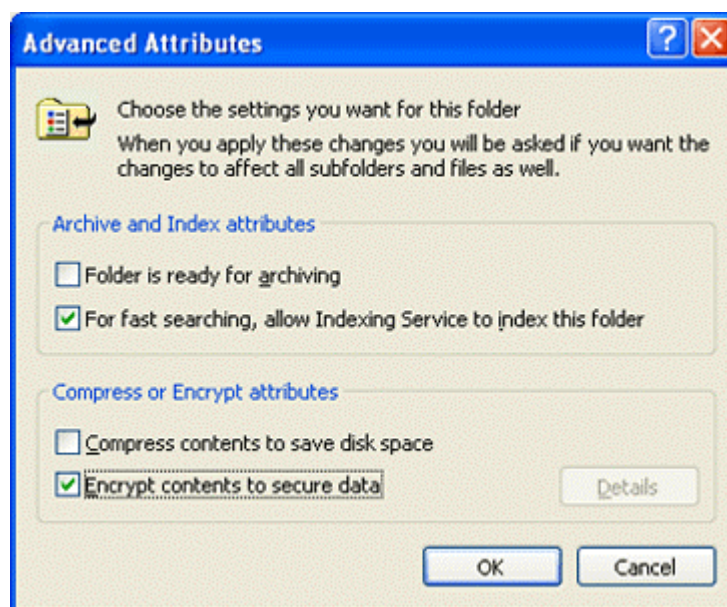


D.6 Encrypted File System

EFS improvements within XP include the 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 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. EFS can be enabled for entire files or folders.

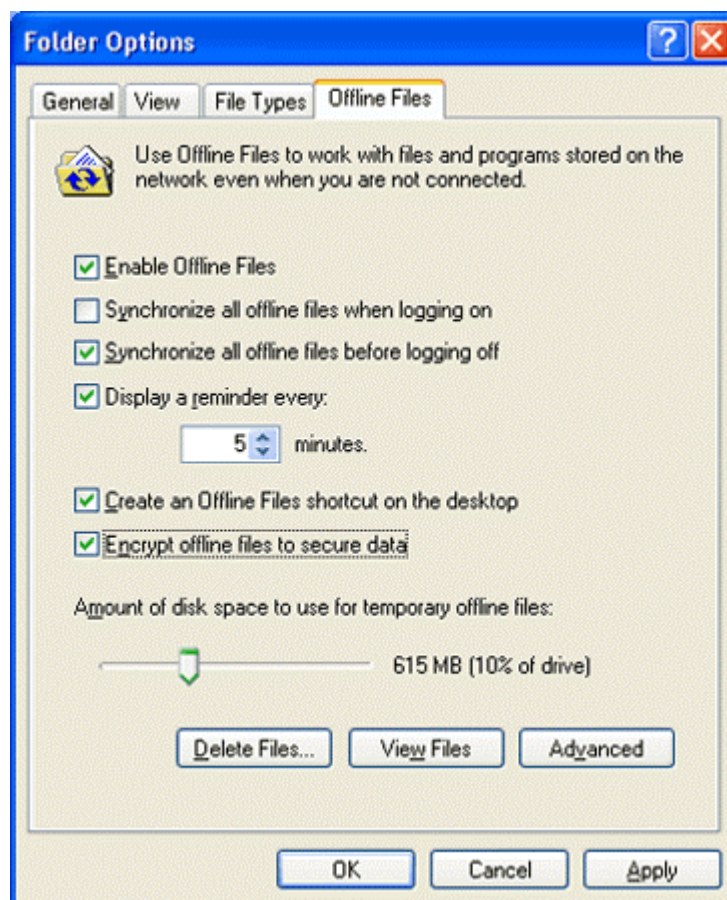
EFS can use either the expanded Data Encryption Standard (DESX) or Triple-DES (3DES) as the encryption algorithm. Both the RSA Base and RSA Enhanced software that cryptographic service providers (CSPs) included in the operating system may be used for EFS certificates, and for encryption of the symmetric 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.

XP EFS Enable Folder Attribute



EFS for XP also works with Offline Folders by encrypting the entire offline files database to protect files used in offline browsing.

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.

Additionally, smart card access can be specifically tied to tools and utilities allowing Administrators to use alternate credentials, so they can do their normal business with normal user privileges, while at the same time being able to carry 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 person guesses the password to an XP machine remotely, he/she will only have guest level access to XP resources.

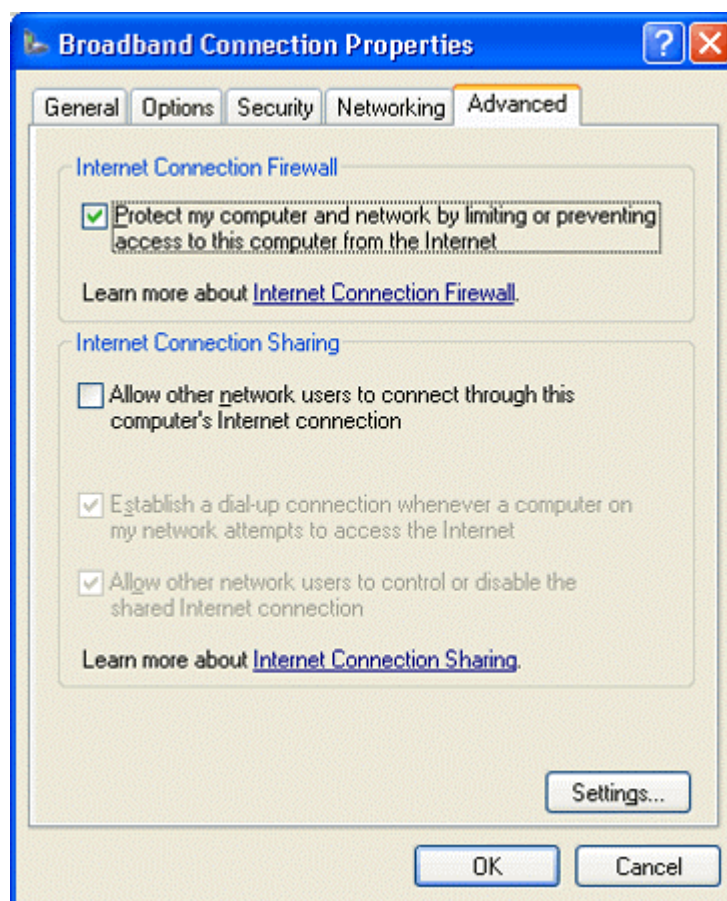
To protect users with non-password protected accounts, Windows XP Professional accounts without passwords can only be used to log on at the physical computer console. By default, accounts with blank passwords can no longer be used to log on to the computer remotely over the network, or for any other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

Note: This restriction does not apply to domain accounts. It also does not apply to the local guest account. If the 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. The ICF is packet inspection software that dynamically opens ports on the firewall for as long as needed to enable access 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 is specifically designed for home based broadband connections.

Note: The vast majority of third party firewalls restrict inbound connections as well as application or port based outbound connections. Restriction of outbound connections increases the security of your system and reduces the potential damage it can do to other systems if compromised.

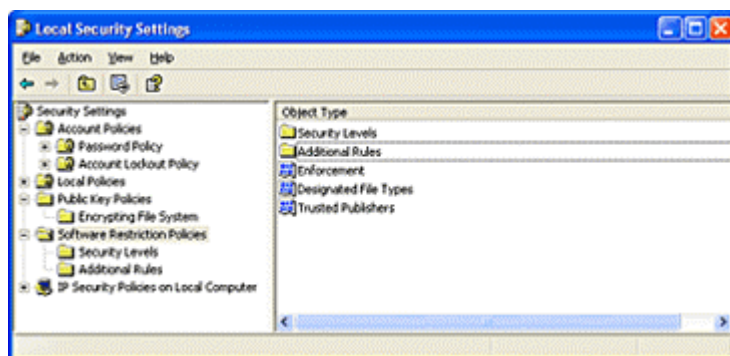
XP ICF Enable Screen**D.10 Software Restriction Policy**

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.

Software Can Be Identified Through One Of The Following Rules:

- Hash rule. A software restriction policy's MMC snap-in allows an administrator 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.

XP Software Restrictions Policy



APPENDIX E: REFERENCES USED IN THIS DOCUMENT

The appendix presents the Internet references used in the creation of this document. The documents listed are excellent resources to use for learning about Windows 2000 security.

References Used in the Creation of this Document

Hyperlink URL	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 Anti-virus solutions within Windows 2000.
http://www.windowssitsecurity.com/Articles/Index.cfm?ArticleID=15741	Article discussing EFS and implementing to secure an install of Windows 2000 on a portable computer.
http://www.windowssitsecurity.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 their infrastructure updates.

Hyperlink URL
Description
http://www.labmice.net/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 on how to create an ERD using Windows Scripting Host (WSH) and JScript.
http://windows2000.about.com/library/weekly/aa040200a.htm Article from about.com discussing creation of ERD and comparisons to Windows NT 4.0
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=15884&Key=Windows%202000%20Professional Discussions of Hotfixes that should be applied to a system that has not yet decided to apply Service Pack 2.
http://www.win2000mag.com/Articles/Index.cfm?ArticleID=15881&Key=Windows%202000%20Professional Additional article discussing hotfixes to apply to a post service pack 1 machine.
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 This article from win2000mag.com discusses a technology new to the upcoming Windows XP, the Windows Client Update and how IE 6 plays into the mix.

Hyperlink URL
Description
http://www.microsoft.com/windows/ie/evaluation/overview/default.asp
<p>From IE 6 Microsoft home page. This is an excellent site to learn more about the technologies specific to IE 6 under the hood.</p>
http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/itsolutions/security/prodtech/wn2ksec.asp
<p>This is a list of Microsoft specific security links for Windows 2000. This will be biased to Microsoft mission.</p>
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&fq=*security%26%22windows%202000%20professional%22
<p>Results of a search for the keywords "Microsoft Windows 2000 professional security" from the Microsoft.com search engine.</p>
http://www.win2000mag.net/Channels/WebAdmin/TopicResults.cfm?TopicID=820
<p>List of links of Windows 2000 topics from an information push channel of win2000mag.com.</p>
http://www.microsoft.com/office/ork/2000/journ/KioskMode.htm
<p>Microsoft.com site for installing Microsoft Office in a public environment. This article discusses privacy issues.</p>
http://support.microsoft.com/support/kb/articles/Q249/3/45.ASP
<p>Microsoft.com knowledge base article on how to secure an install of Microsoft Office on Windows 2000.</p>
http://www.win2000mag.com/Articles/Index.cfm?ArticleID=21577&Key=Windows%202000%20Professional
<p>Article discussing XP product activation codes, this is a new security feature of Office XP.</p>
http://www.win2000mag.com/Articles/Index.cfm?ArticleID=20754&Key=Windows%202000%20Professional
<p>Article discussing pros and cons of upgrading to Office XP.</p>

Hyperlink URL
Description
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=22234&Key=Windows%202000%20Professional
Article discussing Microsoft Personal Security Advisor for windows 2000 professional and how it is not complete yet.
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, mentions secedit.exe binary.
http://www.sans.org/infosecFAQ/win/settings.htm
SANS discussion about the secedit.exe binary and Security Template files.
http://is-it-true.org/nt/nt2000/atips/atips75.shtml
Usage instructions and command line flags for secedit.exe binary.

Hyperlink URL	Description
http://www.shs.ilstu.edu/Windows2000/documents/installation_tools.htm	Document intended to be a resource for administrators 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.zdnet.com/devhead/stories/articles/0,4413,2599160,00.html	ZDNet article for importance of security template files and use of secedit.exe for them.
http://www.zdnet.com/devhead/stories/articles/0,4413,2599163,00.html	ZDNet reference table for previous link containing detailed command line flags for secedit.exe
http://www.win2000mag.com/Articles/Index.cfm?ArticleID=21125&Key=Windows%202000%20Professional	Article discussing the importance of upgrading to Windows 2000 service pack 2.
http://www.wininformant.com/Articles/Index.cfm?ArticleID=21098&Key=Windows%202000%20Professional	Additional article discussing the importance of upgrading to Windows 2000 service pack 2.
http://www.wininformant.com/Articles/Index.cfm?ArticleID=21074&Key=Windows%202000%20Professional	Additional article discussing updated information on the status of Service Pack 2 for Windows 2000. The original reference (also listed here) actually presented false information about service pack 2.
http://www.wininformant.com/Articles/Index.cfm?ArticleID=21051&Key=Windows%202000%20Professional	Additional article discussing updated information on the status of Service Pack 2 for Windows 2000. The original reference (also listed here) actually presented false information about service pack 2.

Hyperlink URL
Description
http://www.win2000mag.com/Articles/Index.cfm?ArticleID=20517&Key=Windows%2000%20Professional
<p>Article regarding upgrade possibilities and requirements to upgrade your Windows 2000 client to Windows XP.</p>
http://www.win2000mag.com/Articles/Index.cfm?ArticleID=21758&Key=Windows%2000%20Professional
<p>Article discussing advancements to Windows XP and how they benefit installation tasks.</p>
http://www.wired.com/news/print/0,1294,42907,00.html
<p>News story from wired.com regarding release of Windows XP.</p>
http://support.microsoft.com/support/kb/articles/Q234/9/26.ASP
<p>Microsoft support article about the sample security templates that ship with Windows 2000.</p>
http://www.sans.org/infosecFAQ/win2000/standalone.htm
<p>SANS article that describes steps to harden/"lock down" a stand-alone Windows 2000 Professional system.</p>
http://www.labmice.net/articles/securingwin2000.htm
<p>LabMice checklist/article for steps to secure an installation of Windows 2000 professional</p>
http://www.labmice.net/install/installbasics.htm
<p>Additional LabMice information for installation instructions of Windows 2000 professional</p>
http://support.microsoft.com/support/kb/articles/Q249/1/49.ASP
<p>Microsoft Tip for installing Windows 2000 along with Windows hotfixes in one step</p>
http://help.netscape.com/communicator/install_guide.html
<p>Installation guide for Netscape 4.78 and later versions on Windows 2000</p>

Hyperlink URL
Description
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 This article describes the 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 This is a 2-part article discussing changes in NTFS 5.0 within Windows 2000 including advancements to ACL control.
http://www.bugnet.com/alerts/ba0105171.html This is an article review on the installation process of Windows 2000 service pack 2.
http://www.sans.org/infosecFAQ/e-mail/sec_outlook.htm This is 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 This resource details how to remove the VBS extensions from the known list. This safeguards against VBS worms and viruses.
http://www.eudora.com The Web site for the Eudora e-mail program
http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci214077,00.html whatis.com page for the LDCM from Intel

Hyperlink URL
Description
http://www.Webopedia.com/TERM/L/LDCM.html
More on LDCM
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

This section 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 Administrators Guidance for Windows 2000 Professional Systems document.

While there are thousands of Internet sites that do provide valuable security information for the Windows 2000 operating system and other Microsoft products. This list is aimed at those Internet sites that strive to provide security-centered reference services.

Computer Security Links

Hyperlink URL
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 as 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

Hyperlink URL
Description
<p>http://www.activewin.com/win2000/index.shtml</p> <p>This is a Microsoft sponsored site containing vulnerability information and associated patch information.</p>
<p>http://www.cert.org</p> <p>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.</p>
<p>http://www.labmice.net</p> <p>A Windows 2000 resource index that contains links to internal and external documents written on a variety of topics relating to Windows 2000</p>
<p>http://www.microsoft.com/technet/</p> <p>Home of Microsoft reference site for non-development technologies of Microsoft product line. This site provides extremely valuable information on Windows 2000 Professional.</p>
<p>http://www.microsoft.com/windows2000</p> <p>The Microsoft Windows 2000 home page. This site is a great starting block for information regarding Windows 2000 security.</p>
<p>http://www.microsoft.com/windows2000/technologies/security/default.asp</p> <p>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 is a Microsoft corporate site and as such can be trusted to be maintained very well. This site should be seen as an index page to specific technology links that are seen below.</p>
<p>http://www.sans.org/infosecFAQ/</p> <p>SANS site for information security reference. This site contains many articles relating directly to Windows 2000 that you can find simply by searching for.</p>

Hyperlink URL
Description
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.
http://www.windowsitlibrary.com Informative reference site for Windows product line. NOTE: this site is a 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 does provide 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 is a service of Internet Security Services and 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 A-2 presented the list of reference materials pertaining to Windows 2000 Professional security and Table A-3 presents the list of major book publishing companies that have been referenced.

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

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

Title		
Author	Publisher	ISBN

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

Title		
Author	Publisher	ISBN

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

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

Title		
Author	Publisher	ISBN

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 shows publishers that have been cited for their works on Windows 2000 Professional security.

Table A-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/

Publisher	Internet URL
McGraw Hill	http://www.mcgraw-hill.com/