

**UNCLASSIFIED**

Report Number: C4-008R-99

---

# **Guide to Securing Microsoft Windows NT<sup>®</sup> Networks**

**Network Attack Techniques Division  
of the  
Systems and Network Attack Center (SNAC)**

**Authors:**

Paul F. Bartock  
LT William J Billings, USN  
Julie M. Haney  
LCDR Frank Q. Meza, USN  
CW02 Denis Mermod, USN  
Warren F. Shadle  
2Lt Robin G. Stephens, USAF



Updated: March 1, 1999  
Version 2.1

National Security Agency  
9800 Savage Rd. Suite 6704  
Ft. Meade, MD 20755-6704

410-854-6529

**UNCLASSIFIED**

**UNCLASSIFIED**

This Page Intentionally Left Blank

**UNCLASSIFIED**

**(U) Warnings**

- **(U) Do not attempt to install any of the settings in this guide without first testing in a non-operational environment.**
- (U) This document is only a guide containing recommended security settings. It is not meant to replace well-structured policy or sound judgment. Furthermore this guide does not address site specific configuration issues. Care must be taken when implementing this guide to address these issues such as the use of products like Microsoft Exchange, IIS, and SMS.
- (U) The security changes described in this document only apply to Microsoft Windows NT 4.0 Service Pack 4 systems and should not be applied to any other Windows NT versions or operating systems.
- (U) You can severely impair or disable a Windows NT system with incorrect changes or accidental deletions when using programs (Examples: Security Configuration Manager, Regedt32.exe, and Regedit.exe) to change the system configuration. Therefore, it is extremely important to test all settings recommended in this guide before installing them on an operational network.
- (U) Currently, there is no Undo command for deletions within the registry. The registry editor prompts you to confirm the deletions if "Confirm On Delete" is selected from the options menu. When you delete a registry key, the message does not include the name of the key you are deleting. Therefore, check your selection carefully before proceeding with any deletion.
- (U) SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE EXPRESSLY DISCLAIMED. IN NO EVENT SHALL THE CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
- (U) This document is current as of February 15, 1999. See <http://www.microsoft.com> for the latest changes or modifications to the Windows NT operating system.

UNCLASSIFIED

This Page Intentionally Left Blank

UNCLASSIFIED

**(U) Acknowledgements**

(U) The authors would like to acknowledge the authors of the "*Guide to Implementing Windows NT in Secure Network Environments*".

**(U) Trademark Information**

(U) Microsoft, MS-DOS, Windows, Windows NT, Windows 98, Windows 95, Windows for Workgroups, and Windows 3.1 are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and other countries.

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

**(U) Table of Contents**

**(U) Warnings ..... iii**

**(U) Acknowledgements..... iv**

**(U) Trademark Information ..... vi**

**(U) Table of Contents ..... vii**

**(U) Table of Figures..... xii**

**(U) Table of Tables ..... xiii**

**(U) Introduction..... 1**

*(U) Getting the Most from this Guide..... 1*

*(U) About the Guide to Securing Microsoft Windows NT Networks ..... 2*

**(U) Chapter 1 Windows NT 4.0 Overview ..... 5**

*(U) Windows NT Security Architecture ..... 5*

        (U) Security Identifiers (SIDs) ..... 5

        (U) Objects ..... 6

        (U) Access Control List (ACL) ..... 6

        (U) Local Security Authority (LSA) ..... 6

        (U) Security Account Manager (SAM) ..... 6

        (U) Security Reference Monitor (SRM) ..... 6

*(U) Workgroups and Domains ..... 7*

        (U) Workgroups..... 7

        (U) Domains ..... 8

*(U) Single Master Domain Model..... 8*

*(U) Multiple Master Domain Model ..... 9*

**(U) Chapter 2 Windows NT Pre-Configuration Recommendations ..... 11**

*(U) Windows NT 4.0 Installation Recommendations ..... 11*

*(U) File System Selection ..... 11*

        (U) Steps needed to convert the system drive to NTFS: ..... 12

*(U) Physical Security ..... 12*

        (U) Controlling Access to the Site ..... 12

        (U) Controlling Access to Computers ..... 12

        (U) Controlling Access to the Network..... 13

        (U) Controlling Access to Software ..... 13

**(U) Chapter 3 Installing Service Pack 4, Hotfixes, and the Security Configuration Manager ..... 15**

*(U) Service Pack 4 Pre-installation Checklist ..... 15*

*(U) Service Pack 4 Pre-installation Registry Changes ..... 16*

        (U) Adding a Registry Key to Restrict Remote Registry Access ..... 16

        (U) Removing Old Hotfix Registry Entries ..... 17

*(U) Service Pack 4 Pre-installation File System Changes ..... 18*

        (U) Removing Old Hotfix Uninstall Folders ..... 18

# UNCLASSIFIED

(U) <i>Installing Service Pack 4</i> .....	18
(U) Y2Ksetup.exe versus Update.exe .....	18
(U) Y2Ksetup .....	18
(U) Update .....	18
(U) Creating An Uninstall Directory .....	19
(U) Installing Service Pack 4 from a Compact Disk .....	19
(U) Installing the Service Pack from a Network Drive .....	19
(U) Downloading and Extracting the Service Pack from the Internet.....	20
(U) Reapplying Service Pack 4 .....	20
(U) Removing Service Pack 4 .....	21
(U) <i>Post Service Pack 4 Hotfixes</i> .....	21
(U) Manual Installation of Recommended Hotfixes .....	22
(U) To download and extract subsequent hotfixes:.....	22
(U) To install a hotfix:.....	22
(U) Automatic Installation of Recommended Hotfixes.....	22
(U) Applying Hotfixes Along With Service Pack 4 .....	22
(U) How to use Hotfix with Update .....	22
(U) Modifying the Master Hotfix.inf File .....	24
(U) Reapplying Post Service Pack 4 Hotfixes .....	24
(U) Removing Hotfixes .....	24
(U) To remove individually installed hotfixes:.....	24
(U) To remove hotfixes installed as a group:.....	24
(U) <i>Installing the Security Configuration Manager</i> .....	25
(U) To install the SCM GUI and command line tools: .....	25
(U) New Inheritance Model.....	25
<b>(U) Chapter 4 Security Configuration Manager.....</b>	<b>27</b>
(U) <i>SCM Functionality</i> .....	27
(U) The SCM GUI .....	27
(U) The SCM Command Line Tool.....	28
(U) <i>Loading the SCM Snap-in into the MMC</i> .....	28
(U) <i>Security Configuration Files</i> .....	28
(U) <i>Editing Security Configuration Files</i> .....	30
<b>(U) Chapter 5 Modifying Security Configuration Files .....</b>	<b>31</b>
(U) <i>Account Policy</i> .....	31
(U) Account Policy Overview .....	31
(U) Modifying Account Policy via the Security Configuration Manager.....	31
(U) Password Policy Settings .....	32
(U) Account Lockout Policy .....	34
(U) <i>Local Policy</i> .....	35
(U) Auditing Policy .....	36
(U) User Account Auditing .....	36
(U) User Rights Assignment.....	37
(U) Modifying the standard and advanced user rights: .....	37
(U) Special Consideration for an IIS Server .....	40
(U) Security Options .....	41
(U) <i>Event Logs</i> .....	45
(U) Modifying the Event Log Settings via the Security Configuration Manager .....	45
(U) Managing the Event Logs.....	47
(U) Saving And Clearing the Audit Logs.....	47

# UNCLASSIFIED

(U) Resetting the Audit Log Settings After the System Halts .....	47
(U) <i>Restricted Groups</i> .....	48
(U) Modifying Restricted Groups via the Security Configuration Manager .....	48
(U) <i>Services</i> .....	49
(U) Modifying System Services via the Security Configuration Manager .....	49
(U) <i>Registry</i> .....	51
(U) Modifying Registry settings via the Security Configuration Manager .....	51
(U) Modifying Permissions on a Registry Key .....	51
(U) Adding registry keys to the security configuration .....	52
(U) Excluding registry keys from the security configuration .....	52
(U) Recommended Registry Key Permissions .....	53
(U) <i>File System</i> .....	58
(U) NTFS Overview .....	58
(U) Modifying File System settings via the Security Configuration Manager .....	58
(U) Modifying Permissions on a File or Folder .....	59
(U) Adding files or folders to the security configuration .....	59
(U) Excluding files or folders from the security configuration .....	60
(U) Recommended File and Folder Permissions .....	60
Special Consideration for an IIS Server .....	60
<b>(U) Chapter 6 Running Security Configuration Files .....</b>	<b>65</b>
(U) <i>SCM Databases</i> .....	65
(U) <i>SCM Command Line Options</i> .....	66
(U) <i>Performing a Security Analysis</i> .....	67
(U) Performing a Security Analysis via the Command Line .....	67
(U) Performing a Security Analysis via the GUI .....	67
(U) <i>Configuring a System</i> .....	67
(U) Configuring a System via the Command Line .....	67
(U) Configuring a System via the GUI .....	68
<b>(U) Chapter 7 Manual Settings .....</b>	<b>69</b>
(U) <i>Manual Registry Changes</i> .....	69
(U) Running the Registry Editor .....	69
(U) Disabling CDRom Autorun .....	69
(U) Removing Registry Keys .....	70
(U) Removing Subsystem Registry Keys .....	70
(U) <i>Manual Folder and File Permission Changes</i> .....	70
(U) Setting Folder and File Permissions .....	70
(U) Recommended File and Folder Permissions .....	71
(U) Removing Existing Folders and Files .....	72
(U) <i>Share Permissions</i> .....	72
(U) Setting Share Permissions .....	72
(U) Share Security Recommendations .....	73
(U) <i>Auditing</i> .....	73
(U) File System Auditing .....	73
(U) Auditing Registry Changes .....	75
(U) Managing the Event Logs .....	76
(U) Saving and Clearing the Event Logs .....	76
(U) Resetting the Event Log Settings after the System Halts .....	76
<b>(U) Chapter 8 Disaster Recovery .....</b>	<b>79</b>

# UNCLASSIFIED

(U) <i>Emergency Repair Disk</i> .....	79
(U) Modifying Window NT 4.0 Setup Disk for Use with a Post Service Pack 4 ERD.....	79
(U) Creating an Emergency Repair Disk .....	80
(U) Recovering the System Using an Emergency Repair Disk.....	80
(U) <i>Application Problems</i> .....	81
(U) General Application Troubleshooting .....	81
(U) <i>Domain Backup Policy</i> .....	81
(U) Security Implications.....	82
<b>(U) Chapter 9 Network Security</b> .....	<b>83</b>
(U) <i>Default Network Protocols</i> .....	83
(U) <i>Configuring Network Components</i> .....	83
(U) Adding Workstations/Servers to the Domain .....	83
(U) Configuring Network Protocols.....	84
(U) <i>Remote Access Service</i> .....	86
(U) RAS Authentication .....	87
(U) RAS Link Encryption.....	87
(U) RAS Dial-Back.....	87
(U) Secure Configuration of RAS .....	87
(U) RAS Permissions.....	89
(U) Point-to-Point Tunneling Protocol.....	90
(U) RAS Auditing .....	90
(U) <i>Other Network Security Concerns</i> .....	91
(U) FTP Server Service .....	91
(U) DNS Server Service .....	91
(U) Telnet Server Service.....	92
(U) Controlling Network Access .....	92
<b>(U) Appendix A Windows NT 4.0 Service Pack 4 Readme File</b> .....	<b>93</b>
<b>(U) Appendix B List of Bugs Fixed in Windows NT 4.0 Service Packs</b> .....	<b>131</b>
<b>(U) Appendix C Windows NT 4.0 Post Service Pack 4 Hotfix Information</b> .....	<b>151</b>
Master Hotfix.inf.....	151
RPC-Hotfix.....	157
TCP-Hotfix .....	160
Sms-Hotfix .....	161
Clik-Hotfix .....	162
<b>(U) Appendix D PDC.inf</b> .....	<b>163</b>
<b>(U) Appendix E BDC.inf</b> .....	<b>169</b>
<b>(U) Appendix F MemberServer.inf</b> .....	<b>175</b>
<b>(U) Appendix G Workstation.inf</b> .....	<b>181</b>
<b>(U) Appendix H Exchange.inf</b> .....	<b>187</b>
<b>(U) Appendix I IIS_Sample.inf</b> .....	<b>193</b>
<b>(U) Appendix J Microsoft Windows 95/98 Client Information</b> .....	<b>199</b>
(U) What kind of logon security is needed?.....	199
(U) What kind of resource protection is needed on Microsoft networks?.....	199
(U) What kinds of access rights will users have to resources protected by user-level security? ...	199

# UNCLASSIFIED

(U) How do is user-level security enabled? .....	200
(U) Should password caching be allowed?.....	200
(U) Should users be able to change Control Panel settings?.....	200
(U) Does a client hard disk need extra protection?.....	200
(U) Are there applications that should not be run? .....	200
(U) Do certain processes of an application need protection? .....	200
(U) Other system policy issues. ....	200
<b>(U) Appendix K Example Logon Banner .....</b>	<b>203</b>
<b>(U) Appendix L References .....</b>	<b>205</b>

**(U) Table of Figures**

Figure 1 Workgroup Model .....7  
Figure 2 Domain Model Implementation .....8  
Figure 3 Master Domain Model.....9  
Figure 4 Multiple Master Domain Model .....10  
Figure 5 Password Policy Recommended Settings .....33  
Figure 6 Account Lockout Policy Recommended Settings .....35  
Figure 7 Recommended Audit Policy .....36  
Figure 8 Recommended User Rights .....40  
Figure 9 Event Log Recommended Configuration.....46  
Figure 10 System Services Recommended Settings .....50  
Figure 11 Auditable Events.....74  
Figure 12 Registry Key Auditing Dialog Box.....75  
Figure 13 Identification Tab of Network Window .....84  
Figure 14 Protocols Tab of Network Window .....85  
Figure 15 TCP/IP Properties Window.....85  
Figure 16 Advanced IP Addressing Window .....86  
Figure 17 Windows NT Server RAS Network Configuration .....88  
Figure 18 RAS Server TCP/IP Configuration Window.....89

**(U) Table of Tables**

Table 1 Workgroup Model .....	7
Table 2 Component Sections of Master Hotfix.inf File .....	24
Table 3 Microsoft Security Configuration Files.....	29
Table 4 Enhanced Security Configuration Files .....	30
Table 5 Password Policy Options.....	34
Table 6 Account Lockout Policy Options.....	35
Table 7 Recommended User Rights .....	40
Table 8 Recommended Security Options Configuration .....	44
Table 9 Recommended Event Log Settings.....	46
Table 10 Recommended Registry Settings.....	57
Table 11 Recommended File System Settings .....	64
Table 12 Recommended File Folder Permissions .....	71
Table 13 Recommended Printer Share Settings.....	73
Table 14 Registry Audit Events .....	76

UNCLASSIFIED

This Page Intentionally Left Blank

UNCLASSIFIED

## (U) Introduction

(U) The purpose of this document is to inform the reader about the Windows NT 4.0 security mechanisms that are available and how these security mechanisms can be implemented in a network environment. It is intended to provide a solid security foundation for any Windows NT 4.0 network by providing step-by-step instruction on how to utilize the built-in security features of the operating system, additional add-on service packs and hotfixes to eliminate known security vulnerabilities. While networks will vary in purpose and scope, this document outlines security policies and procedures that can be adapted for any Windows NT 4.0 network.

(U) The ***Guide to Securing Microsoft Windows NT Networks*** presents detailed information on how to secure a network based Windows NT 4.0 operating system in coordination with Microsoft's current service pack. Specifically, this document addresses the built-in security features and shortfalls of the default Windows NT 4.0 operating system. The following essential assumptions have been made to limit the scope of this document:

- The network consists of machines running Microsoft Windows NT 4.0 and Microsoft Windows 95/98 clients.

**(U) WARNING: Windows 95 and 98 do not support the same level of security as Windows NT 4.0.**

- The machines are Intel architecture.
- Users of this guide have a working knowledge of Windows NT 4.0 installation and basic system administration skills.

(U) This document is intended for Windows NT 4.0 network administrators, but should be read by anyone involved or interested in Windows NT 4.0 or network security.

### (U) Getting the Most from this Guide

(U) The following list is a suggestion for the use of this guide to successfully secure a Windows NT network according to this guide.

**(U) WARNING: This list does not address site specific issues and every setting in this book should be tested on a non-operational network.**

- (U) Read the guide in its entirety. Subsequent chapters build on information and settings discussed in prior chapters. Omitting or deleting steps can potentially lead to an unstable network that will require reconfiguration and reinstallation of software.
- (U) Perform pre-configuration recommendations:
  - Convert FAT partitions to NTFS if necessary. (Chapter 2)
  - Perform a complete backup of your system if this is not a new installation. (Chapter 8)
  - Create new emergency repair disks if this is not a new installation. (Chapter 8)
- Read Service Pack 4 readme.txt file. (Companion CD)
- (U) Install Service Pack 4 via update.exe or use y2ksetup.exe. (Chapter 3)
- (U) Install Y2K fix and Internet Explorer 4.01 Service Pack 1 if Service Pack 4 is installed via update.exe. (Chapter 3)

## UNCLASSIFIED

- (U) If Service Pack 3 and post Service Pack 3 hotfixes were previously installed on system, perform the following actions:
  - (U) Delete the uninstall directory for Service Pack 3.
  - (U) Delete the registry keys pointing to post Service Pack 3 hotfixes.
- (U) Install post Service Pack 4 hotfixes. (Chapter 3)
- (U) Read the Security Configuration Manager readme.txt file. (Companion CD)
- (U) Install the Security Configuration Manager and Management Console. (Chapter 4)
  - Load MMC snap-in for Security Configuration Manager.
- (U) Review security configuration files contained in the companion CD and make changes to security configuration files as required for your specific site. (Chapter 5)
- (U) Apply appropriate security configuration file applicable to each specific system. For example, apply the BDC.inf file for a Backup Domain Controller. (Chapter 6)
- (U) Make the following changes: (Chapter 7)
  - Manual registry changes.
  - Manual file and directory permission changes.
  - Configure share permissions to include printer shares.
  - Implement file and registry auditing.
- (U) Make appropriate security settings for network protocols and services: (Chapter 9)
  - TCP/IP
  - RAS
  - Ensure ports 135, 137, 138, and 139 are blocked at the premise router.
  - Turn off unnecessary services and close all unnecessary ports.

### **(U) About the Guide to Securing Microsoft Windows NT Networks**

(U) This document consists of the following chapters:

(U) **Chapter 1, “Windows NT 4.0 Overview,”** provides an overview of the Windows NT 4.0 operating system. Discusses the characteristics of the operating system, to include the security components that enforce security policies and domain models.

(U) **Chapter 2, “Windows NT Pre-Configuration Recommendations,”** contains recommendations for how to install Microsoft Windows NT, file system selection, backup, physical security, and a Pre-Service Pack 4 installation checklist.

(U) **Chapter 3, “Installing Service Pack 4, Hotfixes, and the Security Configuration Manager,”** contains instructions on how to install Service Pack 4, post-Service Pack 4 hotfixes, and the Security Configuration Manager.

(U) **Chapter 4, “Security Configuration Manager,”** describes how to use the Security Configuration Manager to implement, edit, and create new security configuration files. This chapter also introduces the security configuration files included with this document.

# UNCLASSIFIED

(U) **Chapter 5, “Modifying Security Configuration Files,”** explains how to modify the various configuration (.inf) files included with this guide. This chapter takes a section by section look at the settings found in the files. The sections covered include Account Policy, Local Policy, Event Log, Restricted Groups, Services, Registry, and File System.

(U) **Chapter 6, “Running Security Configuration Files,”** outlines a step by step process on how to decide which files need to be installed and how to install those specific files. The system function and some of the common applications determine this process.

(U) **Chapter 7, “Manual Settings,”** lists settings that need to be changed that can not be accomplished using the Security Configuration Manager.

(U) **Chapter 8, “Disaster Recovery,”** steps the reader through the actions required to create an Emergency Repair Disk and to restore the system from this disk. Also discussed are the domain backup policy and security implications.

(U) **Chapter 9, “Network Security,”** discusses the security implications when connecting Microsoft Windows NT computers to a network. This chapter includes dynamic host configuration protocol (DHCP), trust relationships, router configuration, remote access, and protocol selection.

(U) **Appendix A, “Windows NT 4.0 Service Pack 4 Readme File,”** contains the full readme.txt file from Microsoft’s Service Pack 4.

(U) **Appendix B, “List of Bugs Fixed in Windows NT 4.0 Service Packs,”** contains the full knowledge base article Q150734 listing bugs fixed in each service pack with its corresponding knowledge base article number.

(U) **Appendix C, “Windows NT 4.0 Post-Service Pack 4 Hotfix Information,”** contains a comprehensive list of all post-Service Pack 4 hotfixes for Windows NT 4.0.

(U) **Appendix D, “Primary Domain Controller Security Configuration File (PDC.inf),”** contains a listing of the file and an explanation of the different security fixes within the file.

(U) **Appendix E, “Backup Domain Controller Security Configuration File (BDC.inf),”** contains a listing of the file and an explanation of the different security fixes within the file.

(U) **Appendix F, “Member Server Configuration File (MemberServer.inf),”** contains a listing of the file and an explanation of the different security fixes within the file.

(U) **Appendix G, “Workstation Security Configuration File (Workstation.inf),”** contains a listing of the file and an explanation of the different security fixes within the file.

(U) **Appendix H, “Microsoft Exchange 5.0/5.5 Security Configuration File (Exchange.inf),”** contains a listing of the file and an explanation of the different security fixes within the file.

(U) **Appendix I, “Microsoft Internet Information Server 4.0 Security Configuration File (IIS\_Sample.inf),”** contains a listing of the file and an explanation of the different security fixes within the file.

(U) **Appendix J, “Microsoft Windows 95/98 Client Information,”** contains a description of how to make Microsoft Windows 95 and 98 clients work with secured Microsoft Windows NT 4.0 servers and workstations.

(U) **Appendix K, “Example Logon Banner,”** contains the logon banner that is included in the *Trusted Network Interpretation of the TCSEC* (Document number: NSC-TG-005, 31 July 1987) known as the “Red Book.”

(U) **Appendix L, “References,”** contains a list of resources cited.

UNCLASSIFIED

This Page Intentionally Left Blank

UNCLASSIFIED

## **(U) Windows NT 4.0 Overview**

(U) Windows NT 4.0 is a true, 32-bit, preemptive, multitasking operating system that is designed to provide a robust and secure operating system. Windows NT 4.0 comes in two versions: Windows NT 4.0 Server and Windows NT 4.0 Workstation. Both versions have the familiar Windows 95/98 interface, but beneath the graphical user interface (GUI) is a powerful operating system designed for corporate and high-end users. The Windows NT 4.0 Server can do everything that a Windows NT Workstation can do, and adds a comprehensive set of tools for managing and administering a Windows NT 4.0 network.

### **(U) Windows NT Security Architecture**

(U) The Windows NT Security Architecture permeates the entire operating system. It provides a secure way to control all access to objects, such as files and printers. Access to these objects is checked by the security subsystem to ensure no application or user gains access without proper authorization. The security subsystem includes the following major components: the Local Security Authority (LSA), the Security Account Manager (SAM), the Security Reference Monitor (SRM), and the logon processes. The security subsystem's primary objective is to regulate access to objects. Under Windows NT, an administrator assigns permissions to users and groups to grant or deny access to particular objects. For example, permissions are used to determine if a user is able to read or write to a particular file. Additionally, an administrator can set rights for a user or group to control the actions that a user or group can perform on the computer or domain. The following actions are examples of rights: ability to shut down the system, perform backups, upload and download drivers, and manage audit logs. Below are descriptions of relevant security items.

#### **(U) Security Identifiers (SIDs)**

(U) Within the Windows NT security architecture, users are identified by their unique Security Identifier (SID), not their username. The security subsystem generates a unique SID at the time the account is created. The generated SID is guaranteed to be unique across both time and space—no other user in the system, or any other system, currently has or will have the same SID. Unlike UNIX, where User IDs can be reused, SIDs are entirely unique.

(U) Windows NT generates a SID using a proprietary hashing function based on the current system time, the amount of execution time the current process has used in the user mode, and the computer name or domain name. The Domain name is dependent on whether the account is created within the User Manager or the User Manager for Domains. These three factors in concert with the hashing function provide a SID that is

# UNCLASSIFIED

virtually guaranteed to be unique. If the user belongs to a group, the user will be given a unique SID for that group while still maintaining his or her own unique SID.<sup>1</sup>

## **(U) Objects**

(U) Almost everything in the Windows NT Operating System is represented as an object. This includes memory devices, system processes, threads, and even windows that appear on the desktop. Objects are the key to providing a high level of security in the Windows NT operating system. An object is a self-contained entity that contains its own data and the functions needed to manipulate that data.<sup>2</sup> Objects contain data and information on who or what processes can access that data/resource. These strict controls provide great flexibility for security management.

## **(U) Access Control List (ACL)**

(U) An Access Control List (ACL) is a list of the sets of attributes associated with an object and the users (or SIDs) who may exercise these attributes. The list of attributes and users is represented in a structure known in Windows NT as an Access Control Entry (ACE). Therefore, an ACL is a list of ACEs. Each ACE contains access or auditing permissions to an object for one user or group.

(U) Each object has a pair of ACLs associated with it: a Discretionary ACL, representing rights, which may be assigned, and the System ACL, which is set by the system security policies.

## **(U) Local Security Authority (LSA)**

(U) As the central component of the security subsystem, the Local Security Authority (LSA) generates access tokens, manages security policies on the local computer, and facilitates user logon authentication. The LSA interacts with other parts of the security architecture, such as the SAM, to provide an overall robust and secure system.

## **(U) Security Account Manager (SAM)**

(U) The Security Account Manager maintains a database of all local user and group account information (as well as domain user accounts when in Windows NT server mode). During the logon process, the SAM verifies and identifies users by comparing the authentication data, such as passwords, from its database to data entered by a user. It interacts with the LSA to validate users' requests.

## **(U) Security Reference Monitor (SRM)**

(U) The Security Reference Monitor is the enforcer of the system and the primary element of the security subsystem. This component, fixed in Kernel mode, prevents direct access to objects by any user or process that does not have the proper permissions.

(U) When a user wishes to access a named object, the SRM provides services to check whether the user has the right to access that object. It then provides information on success or failure, and generates any necessary audit messages to be logged by the

---

1 Rutstein, Charles B., *Windows NT Security: A Practical Guide to Securing Windows NT Servers & Workstations*.

2 Sheldon, Tom, *Windows NT Security Handbook*, p. 85.

LSA. Note that although it runs in kernel mode, it responds equally to both user and system authorization requests.<sup>3</sup>

**(U) Workgroups and Domains**

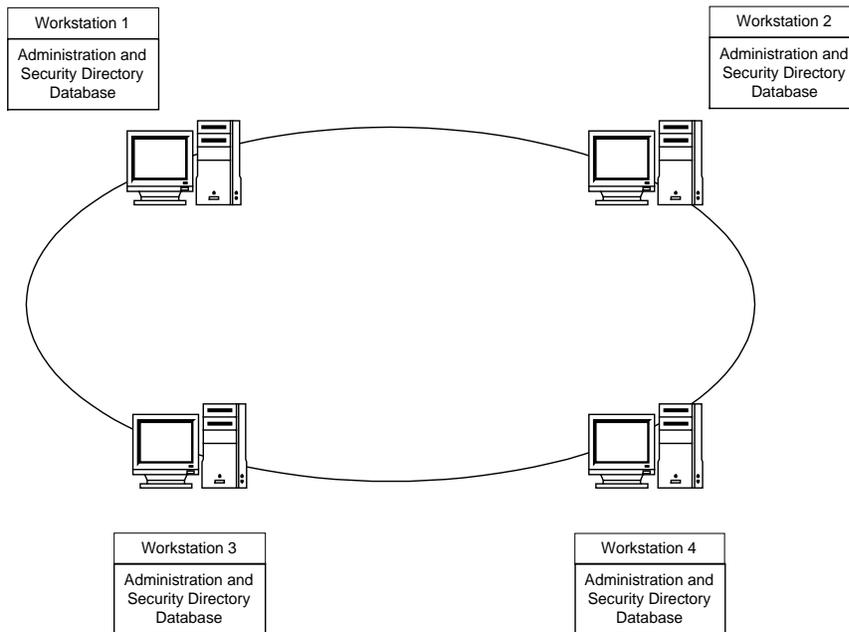
(U) It is important to make an accurate assessment of the needs of an organization prior to selecting a specific network configuration. In Windows NT, the system administrator has the option of implementing the network as a workgroup, a domain, or both.

**(U) Workgroups**

(U) A Workgroup is a collection of computers that are grouped for viewing purposes. An example workgroup configuration is shown in (U) Figure 1. Each workgroup is identified by a unique name. In the workgroup model, each computer functions as both a server and a client, maintaining its own SAM database, performing administration of resources, and enforcing security policies. The workstation's LSA authenticates users for the system from which they log on. The usernames and passwords are checked against that workstation's SAM database. Therefore, in order to gain access to a particular workstation, each user must have a valid account on that machine. The workgroup model provides the following advantages and disadvantages:

ADVANTAGES	DISADVANTAGES
Low cost connectivity Simple design and implementation: No domain controller required	No centralized account management Global security difficult to implement: Must maintain accounts for same user on more than one machine Multiple sources to back up

(U) Table 1 Workgroup Model



(U) Figure 1 Workgroup Model

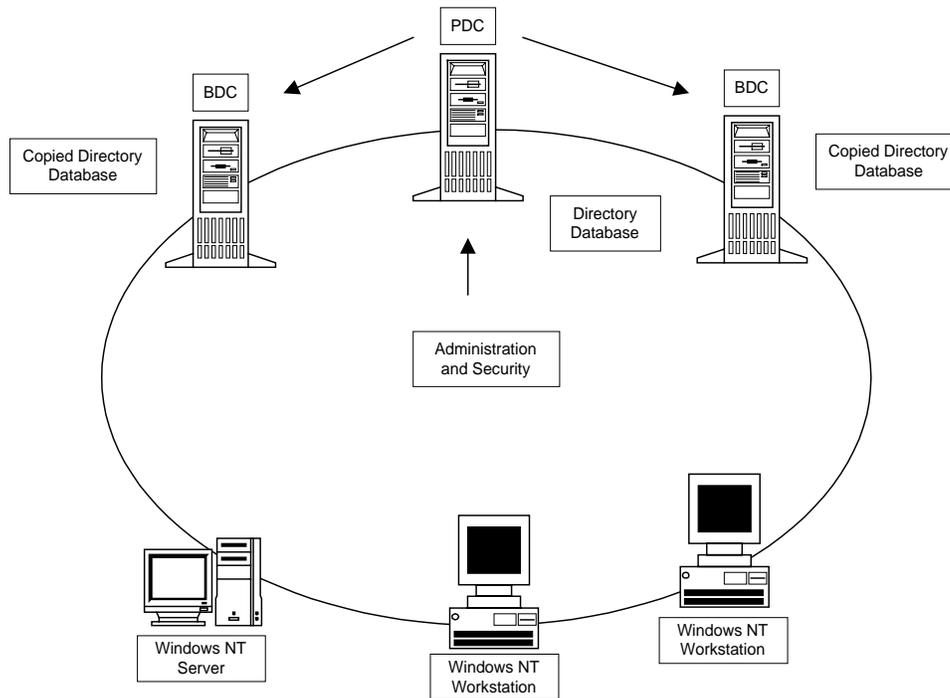
<sup>3</sup> Rutstein, p. 7.

**(U) Domains**

(U) A domain is a collection of computers and users that share a common directory services database. An example domain configuration is shown in

(U) Figure 2. The directory services database allows for central administration of domain account privileges, security, and network resources. The database is stored on the Primary Domain Controller (PDC). The SAM database is periodically replicated to the Backup Domain Controllers (BDC) to increase system reliability and logon response.

(U) By default, domain users automatically have access to all systems participating in the domain. Access to resources is validated against domain SIDs. Every domain user has a unique SID, and every resource has an access list containing SIDs authorized to access that resource.



(U) **Figure 2 Domain Model Implementation**

(U) The advantages of a domain include a single user account for all workstations, universal access to resources, and centralized administration. Additionally, centralized administration of the SAM database enforces a global security policy for all domain users. The domain model provides a centralized approach to sharing network resources and remote administration of the network. System Administrators can use domains to logically split up large networks. This makes it easy for domain users to find needed resources. For example, an administrator can create different user groups with specific job functions, such as Analysts or Managers that use resources exclusive to their own group members.

### **(U) Single Master Domain Model**

(U) The Master domain model designates one domain to manage all user accounts. The master domain also supports global groups. *Global Groups* can export group information to other domains. By defining global groups in the master domain, other domains can

# UNCLASSIFIED

import the group information easily. This model gives you both centralized administration and the organizational benefits of multiple domains.

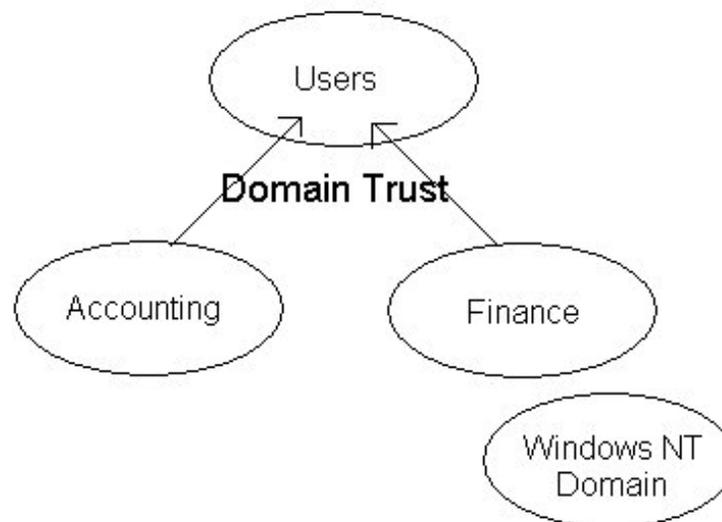
(U) This model balances the requirements for account security with the need for readily available resources on the network because users are given permission to resources based on their master domain logon identity.

(U) The single master domain model is particularly suited for:

- Centralized account management. User accounts can be centrally managed; add/delete/change user accounts from a single point.
- Decentralized resource management or local system administration capability. Department domains can have their own administrators who manage the resources in the department.
- Resources can be grouped logically, corresponding to local domains.

(U) Figure 3 illustrates a network based on a master domain model. The master domain acts as the central administrative unit for user and group accounts. All other domains on the network trust this domain, which means they recognize the users and global groups defined there.

(U) All users log on to their accounts in the master domain. Resources, such as printers and file servers, are located in the other domains. Each *resource domain* establishes a one-way trust with the master (account) domain, enabling users with accounts in the master domain to use resources in all the other domains. The network administrator can manage the entire multiple-domain network and its users and resources by managing only a single domain.



(U) Figure 3 Master Domain Model

## (U) Multiple Master Domain Model

(U) In the multiple master domain model, there are two or more single master domains. Like the single master domain model, the master domains serve as account domains, with every user and computer account created and maintained on one of these master

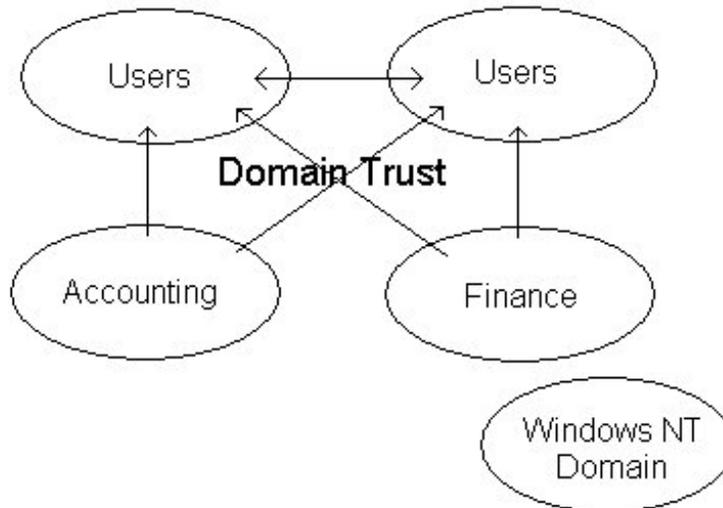
# UNCLASSIFIED

domains. Like the single master domain model, the other domains on the network are called resource domains; they don't store or manage user accounts but do provide resources such as shared file servers and printers to the network.

(U) In this model, every master domain is connected to every other master domain by a two-way trust relationship. Each resource domain trusts every master domain with a one-way trust relationship. The resource domains can trust other resource domains, but are not required to do so. Because every user account exists in one of the master domains, and since each resource domain trusts every master domain, every user account can be used on any of the master domains.

(U) The multiple master domain model incorporates all the features of a single master domain and also accommodates:

- Organizations of more than 40,000 users. The multiple master domain model is scalable to networks with any number of users.
- Mobile users. Users can log on from anywhere in the network, anywhere in the world.
- Centralized or decentralized administration.
- Organizational needs. Domains can be configured to mirror specific departments or internal company organizations.
- BDCs can be distributed between sites to facilitate LAN-WAN interactions.



**(U) Figure 4 Multiple Master Domain Model**

(U) Disadvantages of the multiple master domain model include the following characteristics:

- The numbers of groups and trust relationships multiply rapidly as the number of domains increases.
- User accounts and groups are not located in a single location, complicating network documentation.

## (U) Windows NT Pre-Configuration Recommendations

(U) Before the upgrade software is installed, it is important to make some configuration changes to ensure that the installation is as smooth as possible. Since all installations are different, it is important to back up all computers and test the new software before installing it across a whole network.

(U) Some of the pre-configuration recommendations involve security related system settings that are required before installing the service pack, hotfixes, and the Security Configuration Manager.

**(U) WARNING:** It is extremely important to test hardware and software drivers for compatibility with Service Pack 4. Check the documentation supplied with the drivers and the manufacturer's web page for this information prior to installing any new software or making any recommended changes. If this information is not available it becomes even more critical to test the installation and security settings before installing on an operational network.

### (U) Windows NT 4.0 Installation Recommendations

(U) For the highest level of system integrity, Windows NT 4.0 should be installed on its own partition. Data and applications should be kept separate from the operating system partition.

(U) Any domain model is well suited for large networks or networks that require strong security policies, centralized account management, and flexibility in assigning user rights and permissions. Therefore, it is recommended that all government agencies implement a domain model for their networks.

### (U) File System Selection

(U) All volumes must use the New Technology File System (NTFS) in order to achieve the highest level of security. Under Windows NT, only NTFS supports Discretionary Access Control to the directories and files. NTFS volumes provide secure and auditable access to the files. Therefore, any File Allocation Table (FAT16) partitions must be converted to NTFS. This conversion will not take effect immediately on the system drive or any drives being used for page swapping; in this case it is performed when the system is restarted. This process should not destroy any data.

(U) A non-NTFS volume can be converted at any time using the `Convert.exe` program (`%SystemRoot%\system32\convert.exe`). The `Convert` command must be executed from a command prompt window using an administrative account. The syntax for this command is:

# UNCLASSIFIED

```
CONVERT drive_letter /FS:NTFS [/V]
```

(U) NOTE: The /v switch runs the program in verbose mode.

## (U) Steps needed to convert the system drive to NTFS:

- Select Start → Programs → Command Prompt
- At the command prompt, type:

```
convert c: /FS:NTFS
```

(U) NOTE: Substitute the drive letter of the operating system partition if Windows NT is located on a partition other than C:

(U) At this point the EVERYONE group will have full control of the entire partition. It is critical that stricter file permissions be set before any users are added to the system. The Everyone group includes all users, including anonymous users and null connections.

- Restart system.

## (U) Physical Security

(U) A physical security policy must be formulated and implemented throughout the organization. It is paramount that users understand and adhere to the organization's physical security policy. Educating users of their responsibilities is essential to maintaining a strong physical security posture and preventing inadvertent disclosure of sensitive data to unauthorized personnel.

### (U) Controlling Access to the Site

(U) Physical security measures are needed to protect systems and data from theft, corruption, and natural disasters. Security guards, key-card access systems, and surveillance equipment are critical if the site is open to the public or if information is extremely sensitive. Unauthorized personnel entering the building undetected could gain access to computers, wiring systems, phone systems, and other equipment. Monitoring equipment, such as surveillance cameras, can be installed. Therefore, controlling physical access to the site is the first step.

### (U) Controlling Access to Computers

(U) Files can be modified or hardware tampered with if physical access to computers is not managed properly. To enhance physical security, implement the following security measures:

- Keep servers in a locked room
- Disable the floppy based boot option if available
- Remove the floppy drive if not required or install a locking device
- The CPU case should be secured by a key stored safely away from the computer
- Remove network cards if not required
- Remove modem cards if not required
- Refer to system documentation to implement a power-on bios password

# UNCLASSIFIED

(U) NOTE: Many hardware platforms can be protected using a power-on password. A power-on password prevents unauthorized personnel from starting an operating system. Power-on passwords are a function of the computer hardware, not the operating system software. Therefore the procedure for setting up the power-on password depends on the type of computer and is available in the vendor's documentation supplied with the system.

## **(U) Controlling Access to the Network**

(U) Unauthorized users can access domain resources through unsecured network connections. To enhance network security, implement the following security measures:

- Secure network cables and connections
- Use optical fiber links rather than twisted pair when cabling passes through unsecured areas
- Remove unnecessary systems from the network
- Remove unused cables from the network

## **(U) Controlling Access to Software**

(U) In addition to the physical security policies that limit compromises, implement the following software security measures:

- Resources such as emergency repair disks and backup software should be kept in a secure area.
- Only system administrators should be given the ability to install software
- Software should be inventoried and protected from unauthorized personnel
- Use current virus scanning software to prevent the introduction of malicious code

UNCLASSIFIED

This Page Intentionally Left Blank

UNCLASSIFIED

## (U) Installing Service Pack 4, Hotfixes, and the Security Configuration Manager

(U) Since Windows NT 4.0's introduction, Microsoft has released four service packs. A service pack is a periodic update to the operating system that contains fixes to numerous problems users have experienced. Updates addressing specific problems introduced between service packs are called *hotfixes*. Service packs are cumulative, meaning they include all hotfixes from previous service packs, as well as new fixes.

(U) As of the release of this guide, the latest Windows NT service pack is Service Pack 4. Service Pack 4 includes Internet Explorer 4.01 and addresses several critical operating system issues, including security enhancements. For a brief description of the major security enhancements in Service Pack 4 see Appendix A. Refer to Appendix C for the list of hotfixes current as of this document's release date.

(U) To achieve the highest level of Windows NT security, install Service Pack 4 and the hotfixes recommended in this chapter. For a complete list of available service packs and hotfixes go to <ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/>. It is also important to install any hotfixes for Service Pack 4 that have been released since this guide was written.

(U) Service Pack 4 provides support for a new administrator tool called the Security Configuration Manager (SCM). This tool allows for security analysis and configuration of Windows NT machines. The installation of the SCM will be discussed in this chapter. Chapter 4 provides further details on the use of the SCM.

**(U) WARNING: Test extensively before installing any software on an operational system. Also, Chapter 2 lists many pre-installation recommendations.**

### (U) Service Pack 4 Pre-installation Checklist

(U) The following checklist is designed to provide a simple, easy to follow list to use before installing any software recommended in this book. This checklist does not include any of the physical security recommendations or access control settings.

- (U) Read the Service Pack 4 Readme.txt file (Appendix A) for installation instructions, descriptions of Service Pack 4 fixes and added functionality, and software/hardware incompatibilities.

**NOTE: Taking a few minutes to read the Readme file could save hours in frustration if the software and/or hardware on your system are incompatible with Service Pack 4.**

- (U) Follow Microsoft's eight step pre-installation checklist before installing Service Pack 4:
  - 1) (U) Perform a full backup of files and the registry.

## UNCLASSIFIED

- 2) (U) Update the emergency repair disk (ERD). Use the `rdisk /s` parameter to get the Security and SAM registry hives updated on the disk. For more instructions, see the following Knowledge Base articles:

- Q156328—Description of Windows NT Emergency Repair Disk
- Q122857—`RDISK /S` and `RDISK /S-` Options in Windows NT

(U) **NOTE:** `rdisk /s` can cause serious problems with large SAMs. See Q122857 for more information.

- 3) (U) Perform a full system restart and check the Event Viewer for errors. Resolve any issues before installing SP4.
- 4) (U) Copy your previous Uninstall directory to a safe location. By default, this directory is located in `%SystemRoot%\$NTServicePackUninstall$`.

(U) **NOTE:** Before installing Service Pack 4, it is advised to save the current service pack's uninstall folder. For example, if you remove SP4, the system would be restored to the previous service pack installed (for example, SP3). If you continued to experience problems and wanted to restore the system to a state before SP3, the backup of the older service pack's uninstall folder would allow you successfully remove SP3. Besides retaining the most recoverable system, this will allow tracking the history of the system.

- 5) (U) Run `Srvinfo.exe` from the Windows NT 4.0 Resource Kit and document existing hotfix information.
- 6) (U) Disable any non-essential third-party drivers and services not required for starting the system. Contact the manufacturers about updated versions.
- 7) (U) Verify available disk space. The installation of SP4 requires 40 MB to 80 MB of drive space for the installation, depending on whether the Uninstall option is chosen.
- 8) (U) Close all active debugging sessions or remote control sessions before starting the installation.

- (U) Identify any third party software and verify the software is compatible with Service Pack 4.
- (U) Perform a full backup of your system, including system registry files. A full backup is the only way to restore your system to a previous working installation. See Chapter 12 for information regarding domain backup policy and security implications.

(U) **NOTE:** This step is unnecessary if installing Service Pack 4 onto a new system that does not have any software or data installed.

### (U) Service Pack 4 Pre-installation Registry Changes

#### (U) Adding a Registry Key to Restrict Remote Registry Access

(U) The Registry Editor supports remote access to the Windows NT registry. To restrict network access to the registry, create the following registry key if it does not already exist:

# UNCLASSIFIED

Hive: HKEY\_LOCAL\_MACHINE

Key: \System\CurrentControlSet\Control\SecurePipeServers

Name: winreg

- Run regedt32
- Select HKEY\_LOCAL\_MACHINE in the Local Machine window
- Navigate down the \System\CurrentControlSet\Control\SecurePipeServers path, double clicking on each key along the way

(U) If the **winreg** key exists under SecurePipeServers:

- Highlight the **winreg** key
- Select **Add Value...** from the **Edit** menu
- Enter “**RestrictGuestAccess**” for **Value Name**:
- Select REG\_DWORD from the **Data Type**: drop down list
- Click **OK**
- Enter 1 for the **Data**: value in the DWORD Editor
- Click **OK**

(U) Otherwise, create the **winreg** key and:

- Highlight the **SecurePipeServers** key
- Select **Add Key...** from the **Edit** menu
- Enter “**winreg**” in the **Key Name**: field
- Leave the **Class**: field blank
- Click **OK** to close the **Add Key** window

## (U) Removing Old Hotfix Registry Entries

(U) Previous service packs kept track of hotfixes installed on the system in the HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Hotfix registry key. Service Pack 4 now stores its hotfix entries in HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SP4\Hotfix.

U) Remove the following old Hotfix registry key:

- Run `regedt32.exe`
- Select HKEY\_LOCAL\_MACHINE in the Local Machine window
- Navigate down the \SOFTWARE\Microsoft\Windows NT\CurrentVersion\ path, double clicking on each key along the way
- Select the **Hotfix** key
- Press **Del**
- If confirm on delete is highlighted click **OK**

## (U) Service Pack 4 Pre-installation File System Changes

### (U) Removing Old Hotfix Uninstall Folders

(U) If hotfixes for previous service packs have been installed on the system, uninstall folders for these hotfixes exist. To minimize confusion with post-Service Pack 4 hotfixes and avoid accidentally uninstalling a Service Pack 3 hotfix after Service Pack 4 (SP4) has been installed, these old uninstall folders should be removed prior to installing SP4. For additional information on the problems that could occur if old uninstall folders are not removed, refer to <http://support.microsoft.com/support/kb/articles/q194/33/4.asp>.

(U) Each hotfix uninstall folder is located in %SystemRoot%, the directory in which Windows NT was installed (usually C:\winnt).

- Delete each hotfix uninstall folder in %SystemRoot%

**(U) NOTE: The Hotfix Uninstall folders are preceded with \$NtUninstall. A Q number (Microsoft Knowledge Base article number) or the word HotfixGroup usually follows the \$NtUninstall. For example, a hotfix uninstall folder could be called %SystemRoot%\\$NtUninstallQ156655\$.**

## (U) Installing Service Pack 4

(U) For security reasons, it is recommended that the 128-bit version of Service Pack 4 be installed instead of the 40-bit version. A copy of the 128-bit Service Pack 4 is included on the companion CD and is also available from Microsoft.

**(U) NOTE: The 128-bit version is restricted to U.S. and Canadian sites.**

(U) If you would like to install post Service Pack 4 hotfixes at the same time as the service pack, please first read the **Automatic Installation of Recommended Hotfixes** section later in this chapter.

### (U) Y2Ksetup.exe versus Update.exe

(U) Service Pack 4 includes two installation programs: `y2ksetup.exe` and `update.exe`. These are located in the `i386\update` directory.

#### (U) Y2Ksetup

(U) `Y2ksetup.exe` provides several patches to make some Microsoft applications (e.g. Internet Explorer, DCOM) Y2K compliant. The `y2ksetup.exe` program will install the service pack, then install Internet Explorer 4.01 and DCOM components. There is no uninstall option for `y2ksetup`. Once the service pack has been applied via `y2ksetup`, Service Pack 4 cannot be uninstalled. The `y2ksetup` program can only be applied once.

**(U) WARNING: There is no ability to uninstall the `y2ksetup` program.**

#### (U) Update

(U) The `update.exe` program installs the service pack without installing Y2K patches or IE4.01. If Y2K issues are present on the system, an alert will appear at the end of service pack installation.

# UNCLASSIFIED

(U) When using the Y2K executable (`y2ksetup.exe`) to install the service pack, Internet Explorer 4.01 is automatically installed. If you do not wish to install Internet Explorer 4.01, you must use the `update.exe` service pack installation file instead of `y2ksetup.exe`.

**(U) WARNING: If you do not install Internet Explorer 3.02 or higher, you cannot install the GUI version of the Security Configuration Manager used in this guide.**

(U) Once `y2ksetup` has been run, it cannot be executed again. Therefore, use `update` to reapply Service Pack 4 at a later time.

## **(U) Creating An Uninstall Directory**

(U) If you want to test drivers and overall functionality of the system before applying Y2K patches, an uninstall directory should be created in case the service pack needs to be backed off. The only way to create this uninstall directory is to run the `update.exe` program before running `y2ksetup`.

**(U) WARNING: Do not install the Y2K patches until you are certain that you no longer need to uninstall the service pack.**

(U) When prompted by the `update.exe` program, check the “**Backup up files necessary to uninstall this Service Pack at a later time**” checkbox. The uninstall subdirectory is located in the `%SystemRoot%` directory with the name `$NtServicePackUninstall$`.

(U) The system will need at least 40 MB of free space on the operating system partition to create an uninstall directory.

## **(U) Installing Service Pack 4 from a Compact Disk**

(U) If Service Pack 4 has been obtained from Microsoft on CDROM or via the Companion CDROM associated with this guide, the following checklist can be used:

- Insert the compact disc containing Service Pack 4 into the CD-ROM drive.
- Select **Start** → **Programs** → **Command Prompt** and change directory to the drive letter associated with the CD-ROM drive.
- Change directory to the service pack directory.
- Change directory to `\i386\update`
- Run `y2ksetup.exe` or `update.exe` as appropriate to install the service pack.
- Follow the directions that appear on the screen. See the note above about creating an uninstall directory.

## **(U) Installing the Service Pack from a Network Drive**

(U) If Service Pack 4 is located on a network drive the following checklist can be used:

- Select **Start** → **Programs** → **Command Prompt** and type the command (e.g. `net use`) to connect to the network drive which contains the Service Pack 4 files.
- Change directory to the network drive folder containing the service pack files.
- Change directory to `\i386\update`
- Run `y2ksetup.exe` or `update.exe` as appropriate to install the service pack.

# UNCLASSIFIED

- Follow the instructions that appear on the screen. See the note above about creating an uninstall directory.

## **(U) Downloading and Extracting the Service Pack from the Internet**

(U) If Service Pack 4 is not available on CD-ROM, download the 128-bit version from one of the following sites:

<http://support.microsoft.com/support/ntserver/content/servicepacks>

<http://www.microsoft.com/support/winnt/sp4start.htm>

<http://mssecure.www.conxion.com/cgi-bin/ntitar.pl>

**(U) NOTE: Because the 128-bit version of the service pack is limited to U.S. and Canadian sites only, you will have to proceed through two web pages that will verify if your IP address is from the U.S. or Canada before being able to download the service pack.**

(U) The following checklist will aid in downloading and installing Service Pack 4:

- A full download of the service pack is recommended. When downloading, save the file as 128Sp4.exe. If the file has already been downloaded with its default name of Nph-ntfinal.pl, rename this file to 128Sp4.exe before installation.
- To extract the service pack files and begin installation, change to the directory where you downloaded the service pack and type 128Sp4.exe at the command prompt or double click on the file name in Windows NT Explorer.
- When prompted, specify the directory into which the extracted service pack files will be placed, e.g. C:\Service Pack 4.
- Once extraction is complete, change to the directory where the extracted service pack files are located, e.g C:\Service Pack 4.
- Change directory to \i386\update
- Run y2ksetup.exe or update.exe as appropriate to install the service pack.
- Follow the instructions that appear on the screen. See the note above about creating an uninstall directory.

## **(U) Reapplying Service Pack 4**

(U) The following are recommendations when reinstalling Service Pack 4 after installing new components:

**(U) NOTE: Any post Service Pack 4 installation changes or additions of software/hardware components made to the system which affect the registry or system files require the reapplication of Service Pack 4. This is necessary because files in Service Pack 4 supercede original Windows NT files.**

- If an uninstall directory was previously created (%SystemRoot%\\$NtServicePackUninstall\$), rename this directory or else it will be overwritten. To rename the directory:
  - Select **Start** → **Programs** → **Windows NT Explorer**
  - Right click on the uninstall directory (%SystemRoot%\\$NtServicePackUninstall\$)
  - Select **Rename**

- Rename the directory (e.g.  
%SystemRoot%\\$NtServicePackUninstall\$.old)
- Reinstall Service Pack 4.

(U) NOTE: The Y2K patches need only be installed once; therefore, if you have previously installed the Y2K version of the service pack, run the `update.exe` program versus `y2ksetup.exe` when reapplying Service Pack 4.

## (U) Removing Service Pack 4

(U) The following list contains instructions on how to remove Service Pack 4 from a system and return the system to its state prior to installation:

(U) NOTE: You cannot remove Service Pack 4 if the Y2K patches have been installed. Doing so could lead to unpredictable results. If you have only installed the service pack via `update.exe` without applying the Y2K patches, you can remove the service pack if an uninstall directory had been created prior to the service pack installation. Any hotfixes applied since the last service pack installation should be removed prior to removing Service Pack 4. See the Post Service Pack 4 Hotfixes section below for details on removing hotfixes.

- Select **Start** → **Programs** → **Command Prompt**
- Change directory to the uninstall directory:  
%SystemRoot%\\$NTServicePackUninstall\$\spuninst
- Execute `spuninst.exe`

(U) The `spuninst.exe` program will replace the files updated by Service Pack 4 with the files from the previous installation and will return your registry settings to their pre-Service Pack 4 state.

(U) NOTE: If you install any applications that require Service Pack 4 or have bug fixes contained in Service Pack 4, performing an uninstall could adversely affect those applications.

## (U) Post Service Pack 4 Hotfixes

(U) Since some of the hotfixes overwrite files that other hotfixes modify, install the hotfixes in ascending order of the date/time stamp on the executables. Although Microsoft recommends applying a hotfix only if a system experiences the specific problem the fix addresses, it is recommended that all security-related hotfixes be installed immediately after installation of Service Pack 4. If Service Pack 4 is reapplied at any time, the hotfixes must also be re-installed.

(U) Appendix C contains a list of post-Service Pack 4 hotfixes, along with the software versions containing or affected by a problem, the date of the hotfix, where to download the fix, the size of the compressed executable, and a Microsoft Knowledge Base article number to find out more information about the hotfix. The Microsoft Knowledge Base is located at <http://support.microsoft.com/support>.

(U) As of the publication of this guide, several security-related post-Service Pack 4 hotfixes have been released. Additional hotfixes may address vendor-specific products and should be installed on a case-by-case basis. Please check

<http://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP4> on a regular basis to see if new hotfixes have been released.

(U) You may either install each hotfix individually (see **Manual Installation of Recommended Hotfixes** section below) or install a group of hotfixes all at once (see **Automatic Installation of Recommended Hotfixes** section below).

(U) See **Appendix C** for more detailed information on individual hotfixes.

### **(U) Manual Installation of Recommended Hotfixes**

(U) The companion CD contains only the hotfixes released at the time of guide publication. Therefore, any hotfix for Service Pack 4 released after the release of this guide needs to be downloaded and installed.

#### **(U) To download and extract subsequent hotfixes:**

- Download the self-extracting hotfix executables from Microsoft.
- Using the executable for each particular hotfix along with the /x flag, extract the files for each hotfix. For example, to extract the files for the nprpc hotfix, at the command prompt, type `nprpc-fxi /x`.
- When prompted, enter the name of the directory where the extracted hotfix files will be placed.

#### **(U) To install a hotfix:**

- Change directory to where the hotfix files are located and execute `hotfix.exe`.
- Reboot the system when prompted.

### **(U) Automatic Installation of Recommended Hotfixes**

#### **(U) Applying Hotfixes Along With Service Pack 4**

(U) Since some hotfixes rely on the installation of Service Pack 4, the system administrator's job may become tedious when components requiring reapplication of the service pack are added to the system. To make the system administrator's job more efficient, the `update.exe` utility in Service Pack 4 can be used to update a Windows NT 4.0 installation by automatically installing Service Pack 4 along with a specified group of hotfixes.

(U) The automatic installation of Service Pack 4 and all hotfixes is accomplished by using the files `hotfix.exe` and `hotfix.inf`. If `hotfix.inf` and `hotfix.exe` are detected in a directory called `Hotfix` within the service pack directory `i386` or `alpha` (as appropriate), `update.exe` executes `hotfix.exe`. The system administrator is then given the option of installing the hotfixes directly after installation of Service Pack 4. This procedure requires only one system reboot and omits the tediousness of rebooting after each individual hotfix installation. For more detailed information on automatic hotfix installations, see <http://support.microsoft.com/support/kb/articles/q166/8/39.asp>.

#### **(U) How to use Hotfix with Update**

The companion CD contains Service Pack 4 with automatic installation of hotfixes. However, as new hotfixes are released, you will need to know the procedure for adding the new hotfixes. The following steps only need to be applied when adding a new hotfix to the set of hotfixes on the companion CD.

## UNCLASSIFIED

- (U) Create a directory for each hotfix to be installed.
  - (U) Using the executable for each particular hotfix along with the /x flag, extract the files for each hotfix. For example, to extract the files for the nprpc hotfix, type `nprpc-fxi /x`. This prompts for the directory where the extracted files will be placed. After extraction, there will be a series of fixed component files (.dll and .exe files) as well as an individual `hotfix.exe` and `hotfix.inf` in each hotfix directory.
  - (U) Create a directory (for example `ServicePack4`) that contains the service pack files.
  - (U) For CD-ROM versions of Service Pack 4:
    - Copy the entire `\i386` or `\alpha` directory to the newly created service pack directory.
  - (U) For downloaded versions of Service Pack 4:
    - Expand the Service Pack 4 files by running the self-extracting service pack file, e.g. `128Sp4.exe`, and extracting into the newly created directory.
  - (U) Create a directory under the `ServicePack4\i386` or `ServicePack4\alpha` directory called `Hotfix` and copy `hotfix.exe` and `hotfix.inf` to it. Obtain these files from one of the hotfix directories – the `hotfix.inf` file must be edited later. This `hotfix.inf` file will become the master `hotfix.inf` file.
  - (U) Copy all the fixed component files (.dll, .exe, and .sys files except `hotfix.exe` and `hotfix.inf`) from the individual hotfix directories to the `ServicePack4\i386\Hotfix` directory.
    - (U) WARNING: Be especially careful of hotfixes that replace the same files. Always copy the most recent version of the component file to the Hotfix directory.**
  - (U) Edit the master `hotfix.inf` file to consolidate a group of hotfixes. To do this, examine the individual `hotfix.inf` files in each of the hotfix directories and add the component sections from each to the master `hotfix.inf` file. Refer to Appendix C for a sample master `hotfix.inf` file that includes the hotfixes recommended above.
- (U) Table 2 identifies the component sections in the master `hotfix.inf` file that *may* need to be modified:

[MustReplace.System32.files]	[CopyAlways.System32.files]
[CopyAlways.Drivers.files]	[CopyAlways.Inf.files]
[SystemRoot.files]	[Drivers.files]
[Osldr.files]	[Inf.files]
[Spldrv.files]	[Fonts.files]
[Uniprocessor.Kernel.files]	[Multiprocessor.Kernel.files]
[IIS.files]	[CopyAlways.IIS.files]
[Eudc.files]	[HTR.files]
[IE.files]	[SourceDisksFiles.Alpha]
[IISAdmin.files]	[Server.IIS.Inf.Files]
[Server.Inf.files]	[Workstation.IIS.Inf.Files]
[Workstation.Inf.files]	[SourceDisksFiles]
[SourceDisksFiles.x86]	[Save.Reg.For.Uninstall]
[Strings]	[Product.Add.Reg]

### (U) Table 2 Component Sections of Master Hotfix.inf File

(U) The two variables, HOTFIX\_NUMBER and COMMENT, in the [Strings] section are used to add a key and values in the **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\SP4\Hotfix** registry key. The [Strings] section must include a unique name and a comment describing the hotfixes in the group. Refer to Appendix C for a sample master hotfix.inf file.

- (U) Run Update.exe in the ServicePack4\i386 directory. This installs Service Pack 4 and gives the option of installing the hotfixes.

### (U) Modifying the Master Hotfix.inf File

(U) Before adding hotfixes to or removing hotfixes from a master hotfix.inf file, the current hotfix group must be uninstalled. This is to ensure that the new hotfix can be uninstalled as part of the group of hotfixes. After modifying the master hotfix.inf file, reapply the group of hotfixes.

### (U) Reapplying Post Service Pack 4 Hotfixes

(U) Anytime Service Pack 4 is reapplied, all hotfixes must be subsequently reapplied. See the Reapplying Service Pack 4 section above for more information on reinstalling the service pack.

### (U) Removing Hotfixes

(U) Hotfixes must be removed prior to removing Service Pack 4. Hotfixes must be removed as a group if installed as a group; otherwise, remove hotfixes in the reverse order as applied.

#### (U) To remove individually installed hotfixes:

- Select **Start** → **Programs** → **Command Prompt**
- Change directory to the location of the extracted hotfix installation files.
- Execute `hotfix.exe /y`

#### (U) To remove hotfixes installed as a group:

- Select **Start** → **Programs** → **Command Prompt**

## UNCLASSIFIED

- Change directory to the location of the group hotfix uninstall files, e.g. `%SystemRoot%\$NTUninstallSP4HotfixGroup$` if the sample `hotfix.inf` included with this guide is used.

- Execute `hotfix.exe /y`

**WARNING:** Removing hotfixes can cause unpredictable results

### **(U) Installing the Security Configuration Manager**

(U) Service Pack 4 supports a new security tool for Windows NT 4.0, the Security Configuration Manager (SCM). The SCM allows an administrator to define and set security settings for Windows NT 4.0 machines through the use of configuration files. The tool also provides for analysis of security settings on a machine prior to security configuration.

(U) Graphical User Interface (GUI) and command-line interfaces are available. Both require that Service Pack 4 be installed prior to SCM installation. The GUI also requires Internet Explorer 3.02 or higher and Microsoft Management Console (MMC) 1.0 or higher. The MMC may be installed during SCM installation.

(U) It is recommended that the command line interface be installed along with the GUI version. The command line program allows for applying only specific parts of the SCM configuration file, whereas the GUI only allows for application of the entire configuration file.

(U) The companion CD contains a copy of the SCM. Chapter 4 provides further details on using the Security Configuration Manager.

#### **(U) To install the SCM GUI and command line tools:**

- If the CD-ROM version of Service Pack 4 is available:
  - On the CD, change directory to `\mssce\i386`
- If the CD-ROM version of Service Pack 4 is unavailable:
  - Download the correct version of the SCM (`scesp4i.exe` or `scesp4a.exe`, as appropriate) from <ftp://ftp.microsoft.com/bussys/winnt/winnt-public/tools/scm/>.
  - At the command prompt or from Windows NT Explorer, run the self-extracting file `scesp4i.exe`
- To install both the GUI and command line versions:
  - Run `mssce.exe`.
  - Answer **Yes** to install MMC as part of the SCE installation.
- To install the command line version only:
  - At the command prompt, run `mssce.exe /c`.

#### **(U) New Inheritance Model**

(U) The Security Configuration Manager was originally designed for use with the upcoming Windows 2000 operating system. Therefore, the Windows 2000 ACL inheritance model was back-ported to Windows NT 4.0 and is now available with the

## UNCLASSIFIED

SCM. You will notice that the ACL editor for files and folders appears to be different than before.

(U) Within the new inheritance model, permissions on child objects are automatically inherited from their parent. This can be seen by the check in the **Allow inheritable permissions from the parent to propagate to this object** checkbox in the ACL editor. More permissions can be explicitly defined for a child object in addition to those the child inherits from its parent.

(U) When the checkbox is not checked, the ACLs defined on that object apply only to that object and its children. No permissions are inherited from the parent object.

(U) Within the SCM configuration files, files or folders that you do not wish to inherit permissions from parent objects must either be explicitly listed with desired permissions, or ignored.

(U) For more information on the new inheritance model provided with the SCM, refer to <http://support.microsoft.com/support/kb/articles/q195/5/09.asp>.

## (U) Security Configuration Manager

(U) Service Pack 4 includes support for the Security Configuration Manager (SCM). The SCM allows system administrators to consolidate all security related system settings into a single configuration file (called an `inf` file in this guide because of the file extension `.inf`). These security settings may then be applied to any number of Windows NT machines. It is possible to layer security configuration files to adjust for different software applications and security settings. The current version of the SCM only allows for security settings to be analyzed or applied to the local system.

(U) The SCM allows configuration of the following security areas:

- Account Policies - includes Password Policy and Account Lockout Policy
- Local Policies – includes Audit Policy, User Rights Assignment, and Security Options
- Event Log – includes settings for the event logs
- Restricted Groups – includes membership settings for sensitive groups
- System Services – includes configurations for services such as network transport
- Registry – includes registry key permission settings
- File System – includes file and folder permission settings

(U) This chapter provides a general overview of the SCM and discusses the SCM configuration files included with the companion CD. Chapter 5 covers how to modify the `inf` files, and Chapter 6 describes how to conduct a security analysis and configuration through the SCM.

(U) For more detailed information on the SCM, refer to Microsoft's Technet January, 1999 white paper "*MS Security Configuration Manager for Windows NT 4*" or the SCM Readme file included on the companion CD.

### (U) SCM Functionality

(U) The security configuration manager supports both a graphical user interface (GUI) and a command line tool.

#### (U) The SCM GUI

(U) The SCM graphical user interface is provided as a Microsoft Management Console (MMC) snap-in.

(U) The SCM GUI allows an administrator to:

- Create and/or edit security configuration files
- Perform a security analysis
- Graphically review the analysis results

- Apply a security configuration to a system  
 (U) **NOTE: The SCM GUI requires Windows NT 4.0 with Service Pack 4, Microsoft Internet Explorer 3.02 or higher, and the Microsoft Management Console 1.0 or higher**

(U) The GUI provides different colors, fonts and icons to highlight the differences between the baseline information and the actual system settings. When an analysis or configuration is performed, all security areas within an `inf` are included in the analysis.

**(U) The SCM Command Line Tool**

(U) The SCM command line tool (`secedit.exe`) is all that is needed to:

- Perform a security analysis
- Apply a security configuration to a Windows NT system  
 (U) **NOTE: The SCM command line requires Windows NT 4.0 with Service Pack 4.**

(U) The command line option allows for analysis of individual security areas versus the entire configuration file. Also, analysis results can be redirected to a file for review at a later time. The command line tool is useful for applying predefined configuration files to many systems using distributed systems management tools.

**(U) Loading the SCM Snap-in into the MMC**

(U) The Security Configuration Manager snap-in must be loaded into the Microsoft Management Console. To load the SCM snap-in:

- Run the Microsoft Management Console (`mmc.exe`)
- Select **Console -> Add/Remove Snap-in**
- Click **Add**
- Select **Security Configuration Manager**
- Click **OK**
- Click **OK**

**(U) Security Configuration Files**

(U) The Security Configuration Manager includes a set of pre-defined configuration files for use by the system administrators. These files are located in `%SystemRoot%\Security\Templates` and include:

<b>File Name</b>	<b>Security Level</b>	<b>Platform</b>
Basicwk.inf	Default	Windows NT 4.0 Workstation
Basicsv.inf	Default	Windows NT 4.0 Server
Basicdc.inf	Default	Windows NT 4.0 Domain Controller
Compws4.inf	Compatible	Windows NT 4.0 Workstation/Server
Compdc4.inf	Compatible	Windows NT 4.0 Domain Controller
Securws4.inf	Secure	Windows NT 4.0 Workstation/Server

# UNCLASSIFIED

<b>File Name</b>	<b>Security Level</b>	<b>Platform</b>
Securdc4.inf	Secure	Windows NT 4.0 Domain Controller
Hisecws4.inf	High Security	Windows NT 4.0 Workstation/Server
Hisecdc4.inf	High Security	Windows NT 4.0 Domain Controller
Off97SR1.inf	Installed after Compatible	Windows NT 4.0 Workstation/Server running Office 97 SR1

**(U) Table 3 Microsoft Security Configuration Files**

(U) The Companion CD containing this document also includes a set of security configuration files that comply with the recommendations found in this manual. Refer to the table below in order to choose the file(s) appropriate to your system(s).

<b>File Name</b>	<b>Security Level</b>	<b>Platform</b>
<b>PDC.inf</b> (U) Includes security settings for domain-wide account policy and local policy, as well as for the local registry and file system.	Enhanced	Windows NT 4.0 Primary Domain Controller
<b>BDC.inf</b> (U) Identical settings of PDC.inf, except this file excludes account policy since PDCs replicate this information to BDCs.	Enhanced	Windows NT 4.0 Backup Domain Controller
<b>Workstation.inf</b> (U) Contains settings for a workstation. These settings (in particular the audit policy) can be modified to meet organizational policies and requirements.	Enhanced	Windows NT 4.0 Workstation
<b>MemberServer.inf</b> (U) Applies to standalone servers within the domain.	Enhanced	Windows NT 4.0 Server (non-domain controller)
<b>Exchange.inf</b> (U) This file should be used for systems having Exchange or other applications using administrative service accounts (e.g. SMS, SQL Server). Registry permissions are not locked down as tightly as in other inf files.	Enhanced	Windows NT 4.0 Server running Exchange 5.0 or 5.5, SMS, SQL Server
<b>IIS_Sample.inf</b> (U) Sample file for use with an IIS server. You must edit this file as detailed in Chapter 5 to manual add the names of the IUSR_<computer_name> and IWAM_<computer_name> accounts on the server. It is recommended	Enhanced	Windows NT 4.0 Server running Internet Information Server 4.0.

<b>File Name</b>	<b>Security Level</b>	<b>Platform</b>
that the IIS server be a standalone server not connected to a domain.		

**(U) Table 4 Enhanced Security Configuration Files**

- (U) Copy the configuration files included on the Companion CD to the template directory (%Systemroot%\Security\Templates\).

## **(U) Editing Security Configuration Files**

(U) The security settings of any of the predefined configuration files can be modified. The following steps should be followed to modify a configuration file(s):

- Within the MMC, double-click on the **Security Configuration Manager** node in the left pane
- Double-click the **Configurations** node
- Double-click the default configuration file directory (%Systemroot%\Security\Templates). A list of available configuration files is revealed.
- Double-click on a specific configuration file
- Double-click on a specific security area
- Double click on a security object in the right pane
- Customize the security setting for your environment
- To save the customized configuration file, right-click on the file in the left pane and select **Save**

(U) Chapter 5 details the recommendations for each security area and how to modify the configuration files.

## (U) Modifying Security Configuration Files

(U) Although the security settings recommended in this book have been tested extensively, they could still cause problems with some applications. Every effort was made to secure the system without loss of performance but some operational environments may require functionality that has been intentionally turned off by these configuration files. Therefore the following sections contain information on how to modify the included configuration files. More information can be found in Microsoft's SCM Whitepaper.

**(U) WARNING:** It is extremely important to test any configuration change before it is implemented in an operational environment.

### (U) Account Policy

#### (U) Account Policy Overview

(U) A key component of controlling the security in a Windows NT domain is the proper setting of account policies. Depending on the type of system (e.g. domain controller, workstations, member server), account policy configuration will impact the network differently. When configuring a primary domain controller's account policy, all domain controllers will be impacted because a PDC's password and lockout policy is a domain-wide setting enforced by all domain controllers. Configuring account policies on workstations and member servers only impacts the local password or lockout policy on the machine. To ensure a consistent password and lockout policy throughout the entire domain, you must set the same policy on the primary domain controller (PDC), member servers and workstations. Excluded from this list are the backup domain controllers (BDCs), which will inherit the domain-wide account policy from the PDC.

#### (U) Modifying Account Policy via the Security Configuration Manager

**(U) NOTE:** After making any modifications to the configuration files make sure the changes are saved (See Chapter 4) and then test the changes before installing them on an operational network.

(U) Before Service Pack 4, account policy could only be configured through the User Manager. Now, with Service Pack 4, account policy should be configured via the SCM.

(U) To view account policy settings of an SCM template:

- Double-click on the **Security Configuration Manager** node. This reveals the following folders:

- Database: Not loaded
- Configurations
- Double click on the **Configurations** node
- Double-click on the default configuration file directory:  
(%SystemRoot%\Security\Templates)
- Double-click on a specific configuration file
- Double-click on **Account Policies**

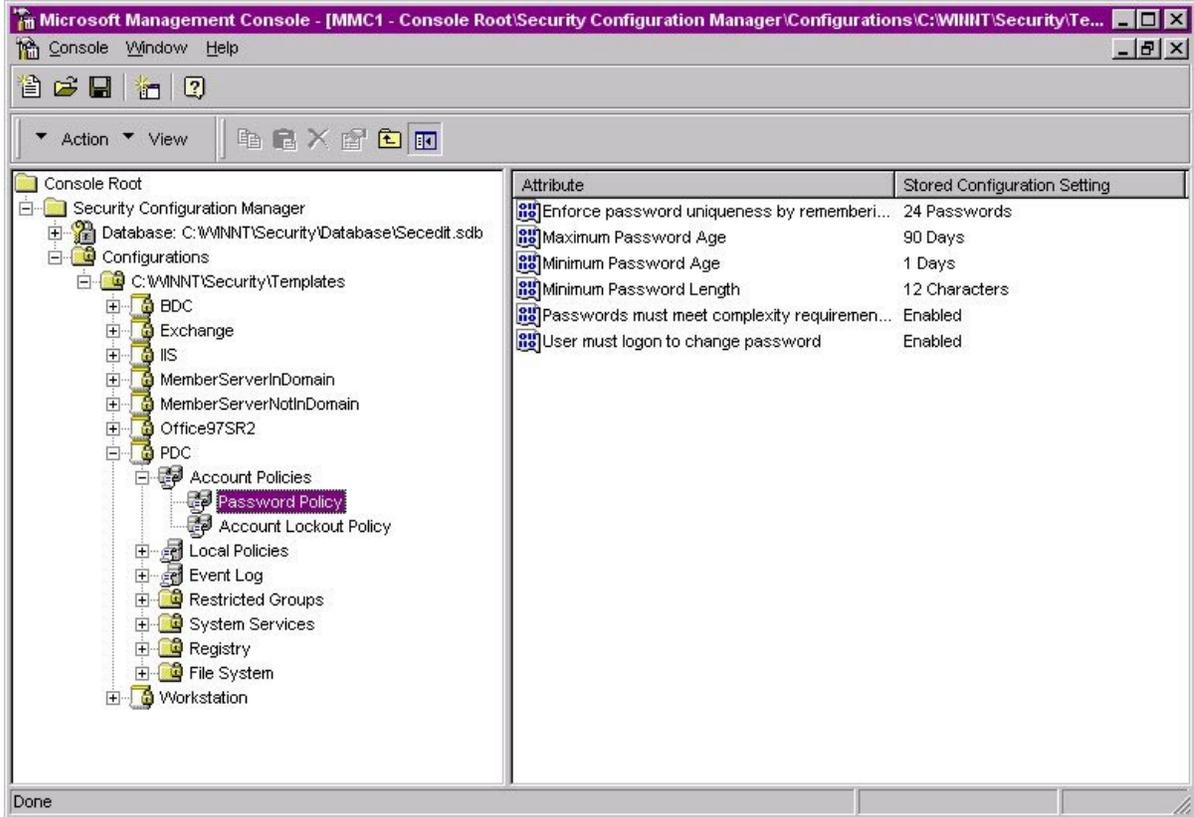
### **(U) Password Policy Settings**

(U) Before making modifications to the **Account Policy** dialog box, review your organization's written password security policy. The settings made in the **Account Policy** dialog box should comply with the written password policy. Users should read and sign statements acknowledging compliance with the organizational computer policy.

(U) Recommendations for a password policy include:

- Users should never write down passwords
- Passwords should be difficult to guess and include uppercase, lowercase, special (e.g. punctuation and extended character set), and numeric characters
- Users should not transmit passwords using any form of electronic communications

**(U) NOTE: After making any modifications to the configuration files make sure the changes are saved (See Chapter 4) and then test the changes before installing them on an operational network.**



(U) Figure 5 Password Policy Recommended Settings

(U) To modify the password policy settings via the Security Configuration Manager, double-click on **Password Policy** under the **Account Policies** node (See (U) Figure 5). Double-click on each of the settings described below to view or edit the current settings. (U) Table 5 list the recommended password policy settings.

<b>Password Policy Options</b>	<b>Recommended Settings</b>
<p><b><u>Enforce password uniqueness by remembering last x passwords</u></b>                      (U) Prevents users from toggling among their favorite passwords and reduces the chance that a hacker/password cracker will discover passwords. If this option is set to 0, users can revert immediately back to a password that they previously used. Allowable values range from 0 (do not keep password history) to 24.</p>	24 Passwords
<p><b><u>Maximum Password Age</u></b>                      (U) The period of time that a user is allowed to have a password before being required to change it. Allowable values include Forever (password never expires) or between 1 and 999 days.</p>	90 days
<p><b><u>Minimum Password Age</u></b>                      (U) The minimum password age setting specifies how long a user must wait after changing a password before changing it again. By default, users can change their passwords at any time. Therefore, a user could change their password, then immediately change it back to what it was before. Allowable values are 0 (allow changes immediately) or between 1 and 42 days.</p>	1 Day
<p><b><u>Minimum Password Length</u></b>                      (U) Blank passwords and shorter-length passwords are easily</p>	12 Characters

Password Policy Options	Recommended Settings
<p>guessed by password cracking tools. To lessen the chances of a password being cracked, passwords should be longer in length. Allowable values for this option are 0 or between 1 and 14 characters.</p>	
<p><b><u>Password must meet complexity requirements of installed password filter</u></b>                      (U) Enforces strong password requirements for all users by use of a dynamic link library called passfilt.dll. Stronger passwords provide some measure of defense against password guessing and dictionary attacks launched by outside intruders. Passwords must contain characters from 3 of 4 classes: upper case letters, lower case letters, numbers, special characters (e.g. punctuation marks). Also, passwords cannot be the same as the user's logon name.                      (U) Complexity requirements will take effect the next time a user changes his password. Already-existing passwords will not be affected.</p>	Enabled
<p><b><u>Users must log on in order to change password</u></b>                      (U) Prevents users from changing their passwords without logging on. If the user's password expires, the user will not be able to log on and an administrator will have to change the user's password.</p>	Enabled

(U) Table 5 Password Policy Options

**(U) Account Lockout Policy**

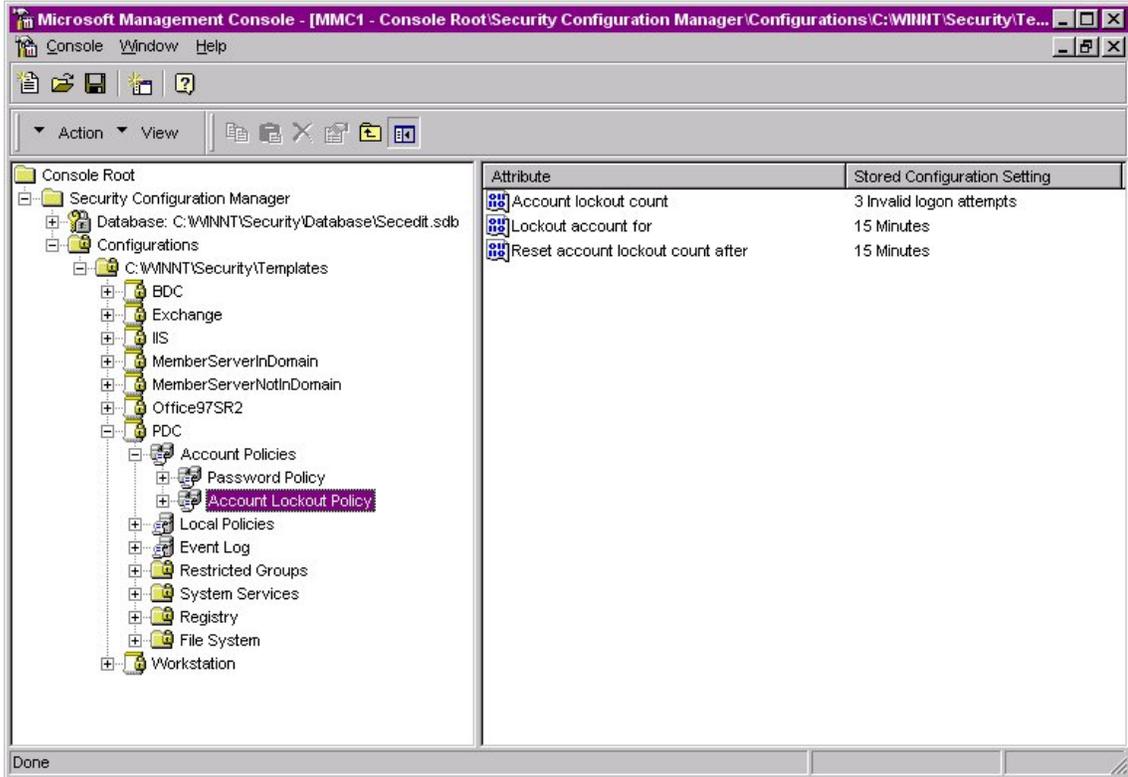
(U) To modify the account lockout policy settings via the Security Configuration Manager, double-click on **Account Lockout Policy** under the **Account Policies** node (See (U) Figure 6). Double-click on each of the settings described below to view or edit the current settings. (U) Table 6 lists the recommended account lockout policy settings.

**(U) NOTE: After making any modifications to the configuration files make sure the changes are saved (See Chapter 4) and then test the changes before installing them on an operational network.**

Account Lockout Policy Options	Recommended Settings
<p><b><u>Account lockout count</u></b>                      (U) Prevents brute-force password cracking/guessing attacks on the system. In a dictionary attack, thousands of well-known passwords are tried. If an account is locked out after several tries, a hacker would have to wait until the account became enabled again, thus slowing down his progress. If an account becomes locked due to hacker attacks or other reasons, an administrator can reset it by using User Manager for Domains.                      (U) This option specifies the number of bad logon attempts that can be made before an account is locked out. Allowable values range from 0 (no account lockout) to 999 attempts.</p>	3 Invalid logon attempts
<p><b><u>Lockout account for</u></b>                      (U) Sets the number of minutes an account will be locked out. Allowable values are Forever (until admin unlocks) or between 1 and 99999 minutes.  <b>(U) WARNING: Setting this value to Forever (until admin unlocks) may allow a potential denial of service attack. It is important to note that the built-in Administrator account cannot be locked</b></p>	15 minutes

Account Lockout Policy Options	Recommended Settings
out.	
<b>Reset account lockout count after</b> (U) Sets the number of minutes until the bad logon count is reset. Allowable values range from 1 to 99999 minutes.	15 minutes

(U) Table 6 Account Lockout Policy Options



(U) Figure 6 Account Lockout Policy Recommended Settings

**(U) Local Policy**

(U) Local Policies also include policy settings that are typically managed from the user manager. These include audit policies and user policies.

(U) To view local policy settings of an SCM template:

- Double-click on the **Security Configuration Manager** node. This reveals the following folders:
  - Database: Not loaded
  - Configurations
- Double click on the **Configurations** node
- Double-click on the default configuration file directory:  
 (%SystemRoot%\Security\Templates)

- Double-click on a specific configuration file
- Double-click on **Local Policies**

**(U) Auditing Policy**

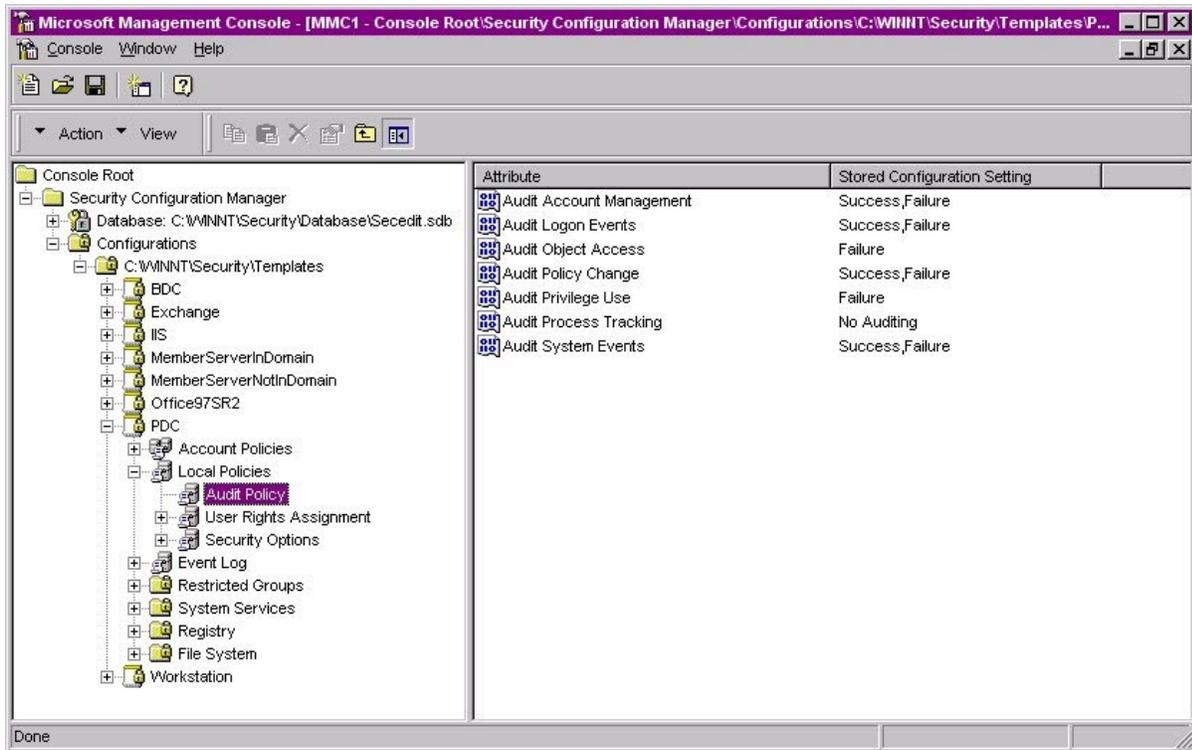
(U) Auditing is critical to maintaining the security of the domain. On Windows NT systems, auditing is not enabled by default, and Audit Policies are set on a per-system basis via the Security Configuration Manager or the User Manager. Each Windows NT system includes auditing capabilities that collect information about individual system usage such as application, system, and security events. The three types of auditing are User Account, File System Auditing and System Registry Auditing. Once System Auditing is enabled, use Windows NT Explorer to set File System Auditing and Regedit32 to set System Registry Auditing.

**(U) WARNING: Auditing can consume a large amount of processor time and disk space. It is highly recommended that administrators check, save, and clear audit logs daily/weekly to reduce the chances of system degradation.**

**(U) User Account Auditing**

(U) Each event that is audited in an audit policy is written to the security event log. The security event log can be viewed with the Event Viewer.

(U) To modify the audit policy settings via the Security Configuration Manager, double-click on **Audit Policy** under the **Local Policies** node (See (U) Figure 6). Double-click on each of the settings shown in (U) Figure 7 below to view or edit the current settings.



**(U) Figure 7 Recommended Audit Policy**

**(U) User Rights Assignment**

(U) User rights are allowable actions that can be assigned to users or groups to supplement built-in abilities. Careful allocation of standard and advanced user rights can significantly strengthen the security of a Windows NT system. The recommended user rights are listed and described in (U) Table 7. These rights are already implemented within the included security configuration files (Shown in (U) Figure 8) and do not have to be modified.

**(U) Modifying the standard and advanced user rights:**

- In the SCM, double-click on **Local Policies**
- Select User Rights Assignment (Shown in (U) Figure 8)
- Double-click the **Attribute** to edit
- Select the **Right** from the pull down menu

(U) To remove a user or group:

- Select the user or group from within the box
- Click the **Remove** button

(U) To add a user or group:

- Click the **Add...** button
- Select the user or group from the **Names** list
- Click the **Add** button
- Click **OK** to continue

**(U) NOTE: After making any modifications to the configuration files make sure the changes are saved (See Chapter 4) and then test the changes before installing them on an operational network.**

UNCLASSIFIED

<b>Standard/Advanced User Rights</b> All shaded areas represent advanced rights	<b>Recommended rights on Windows NT Workstation</b>	<b>Recommended Rights on Windows NT Primary Domain Controller and Member Servers in Domains</b>
<b><u>Access this computer from network</u></b> (U) Allows a user to connect over the network to the computer.	Administrators Authenticated Users	Administrators Authenticated Users
<b><u>Act as part of the operating system</u></b> (U) Allows a process to perform as a secure, trusted part of the operating system. Some subsystems are granted this right.	(None)	(None)
<b><u>Add workstations to the domain</u></b> (U) Allows a user to add workstations to a particular domain. This right is meaningful only on domain controllers. By default, the Administrators and Account Operators groups have the ability to add workstations to a domain and do not have to be explicitly given this right.	(None)	(None)
<b><u>Back up files and directories</u></b> (U) Allows a user to back up files and directories. This right supersedes file and directory permissions	Administrators, Backup Operators Server Operators	Administrators Backup Operators Server Operators
<b><u>Bypass traverse checking</u></b> (U) Allows a user to change directories and access files and subdirectories even if the user has no permission to access parent directories.	(None)	(None)
<b><u>Change the system time</u></b> (U) Allows a user to set the time for the internal clock of the computer	Administrators	Administrators Server Operators
<b><u>Create a pagefile</u></b> (U) Allows a user to create new pagefiles for virtual memory swapping	Administrators	Administrators
<b><u>Create a token object</u></b> (U) Allows a process to create access tokens. Only the Local Security Authority should be allowed create this object.	(None)	(None)
<b><u>Create permanent shared object</u></b> (U) Allows a user to create special permanent objects, such as \\Device, that are used within Windows NT.	(None)	(None)
<b><u>Debug programs</u></b> (U) Allows a user to debug various low-level objects such as threads.	(None)	(None)
<b><u>Force shutdown from a remote system</u></b> (U) Allows a user to shutdown a Windows NT system remotely over a network.	Administrators	Administrators Server Operators
<b><u>Generate security audits</u></b> (U) Allows a process to generate security audit log entries.	(None)	(None)
<b><u>Increase quotas</u></b>	(None)	(None)

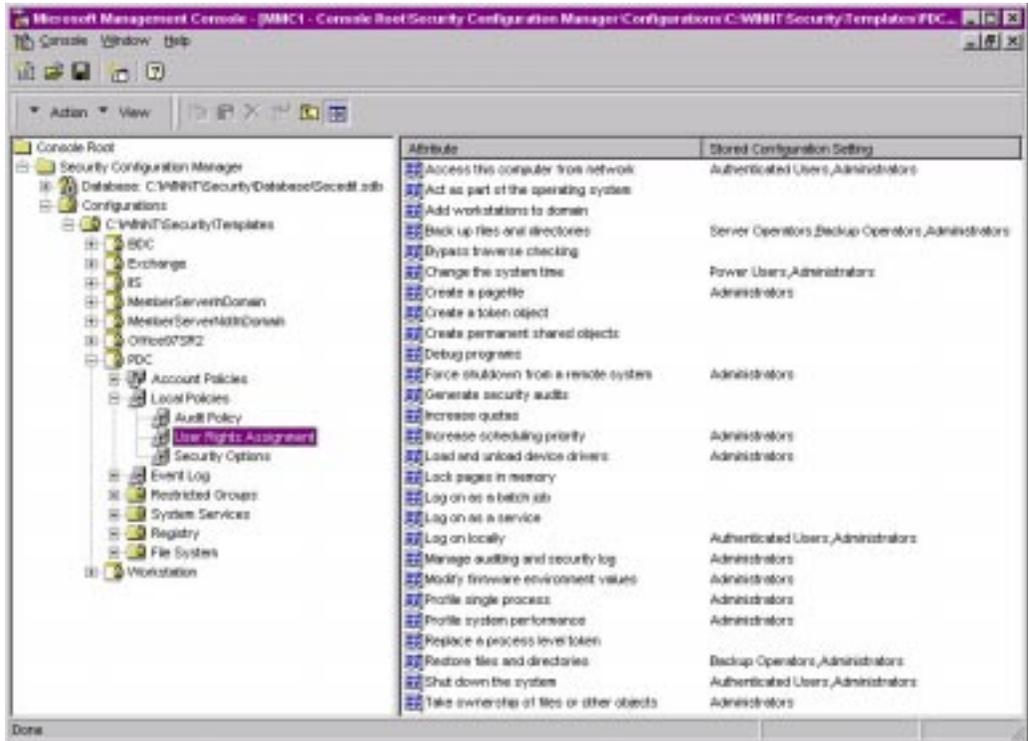
UNCLASSIFIED

<b>Standard/Advanced User Rights</b> All shaded areas represent advanced rights	<b>Recommended rights on Windows NT Workstation</b>	<b>Recommended Rights on Windows NT Primary Domain Controller and Member Servers in Domains</b>
(U) This right has no effect in current versions of Windows NT.		
<b>Increase scheduling priority</b> (U) Allows a user to boost the execution priority of a process.	Administrators	Administrators
<b>Load and unload device drivers</b> (U) Allows a user to install and remove device drivers.	Administrators	Administrators
<b>Lock pages in memory</b> (U) Allows a user to lock pages in memory so they cannot be paged out to a backing store such as Pagefile.sys.	(None)	(None)
<b>Log on as a batch job</b> (U) This right has no effect in current versions of Windows NT.	(None)	(None)
<b>Log on as a service</b> (U) Allows a process to register with the system as a service.	(None)	(None)
<b>Log on locally</b> (U) Allows a user to log on at a system's console.	Administrator Authenticated Users	Administrators Account Operators Backup Operators Server Operators Print Operators
<b>Manage auditing and security log</b> (U) Allows a user to specify what types of resource access (such as file access) are to be audited, and to view and clear the security log. Note that this right does not allow a user to set system auditing policy using the Audit command in the Policy menu of User Manager. Members of the Administrators group always have the ability to view and clear the security log.	Administrators	Administrators
<b>Modify firmware environment variables</b> (U) Allows a user to modify system environment variables stored in nonvolatile RAM on systems that support this type of configuration.	Administrators	Administrators
<b>Profile single process</b> (U) Allows a user to perform profiling (performance sampling) on a process.	Administrators	Administrators
<b>Profile system performance</b> (U) Allows a user to perform profiling (performance sampling) on the system.	Administrators	Administrators
<b>Replace a process-level token</b> (U) Allows a user to modify a process's security access token. This is a powerful right used only by the system.	(None)	(None)
<b>Restore files and directories</b>	Administrators	Administrators

<b>Standard/Advanced User Rights</b> All shaded areas represent advanced rights	<b>Recommended rights on Windows NT Workstation</b>	<b>Recommended Rights on Windows NT Primary Domain Controller and Member Servers in Domains</b>
(U) Allows a user to restore backed-up files and directories. This right supersedes file and directory permissions.	Backup Operators	Server Operators Backup Operators
<b>Shut down the system</b> (U) Allows a user to shut down Windows NT.	Administrators Authenticated Users	Administrators
<b>Take ownership of files or other objects</b> (U) Allows a user to take ownership of files, directories, printers, and other objects on the computer. This right supersedes permissions protecting objects.	Administrators	Administrators

(U) Table 7 Recommended User Rights

NOTE: Based on site policies, some users groups may need to be added or deleted from the recommended User Rights.



(U) Figure 8 Recommended User Rights

**(U) Special Consideration for an IIS Server**

(U) Add IWAM\_<computer\_name> and IUSR\_<computer\_name> and INTERACTIVE to the Log on locally right.

**(U) Security Options**

(U) The SCM Security Option section covers many of the well-known Windows NT security parameters that were previously configured by other utilities such as Regedt32 or Windows NT Explorer. (U) Table 8 lists the recommended settings.

<b>Security Attribute</b>	<b>Recommended Security Setting</b>
<p><b><u>Allow Server Operator to schedule tasks (Domain Controllers Only)</u></b>                      (U)Allows <b>Server Operators</b> to use Schedule Service (AT Command). Or schedule task automatically run at preset time.</p>	Not Configured
<p><b><u>Allow system to be shutdown without having to logon</u></b>                      (U) Normally, you can shut down a computer running Windows NT Workstation without logging on by choosing <b>Shutdown</b> in the <b>Logon</b> dialog box. This is appropriate where users can access the computer's operational switches; otherwise, they might tend to turn off the computer's power or reset it without properly shutting down. However, you can remove this feature if the CPU is locked away. This step is not required for Windows NT Server, because it is configured this way by default.</p>	Disable
<p><b><u>Audit access to internal system object</u></b>                      (U) There are a number of Windows NT system components which are accessible to individuals with programming knowledge that could be used to mount a denial of service attack. To enable stronger protection on these base objects, such as drive letters and printers.</p>	Disable
<p><b><u>Audit use of all user rights including Backup and Restore</u></b>                      (U) Normally, you can shut down a computer running Windows NT Workstation without logging on by choosing <b>Shutdown</b> in the <b>Logon</b> dialog box. This is appropriate where users can access the computer's operational switches; otherwise, they might tend to turn off the computer's power or reset it without properly shutting down. However, you can remove this feature if the CPU is locked away. This step is not required for Windows NT Server, because it is configured this way by default.</p>	Not Configured
<p><b><u>AutoDisconnect: Allow sessions to be disconnected when they are idle</u></b>                      (U) Disconnects a user session from any servers on the domain when it exceeds it's the AutoDisconnect Time.</p>	<Site Specific>
<p><b><u>AutoDisconnect: Amount of idle time required before disconnecting session</u></b>                      (U) Set the amount of elapses idle time allowed before disconnecting the users session.</p>	<Site Specific>
<p><b><u>Change Administrator account name to</u></b>                      (U) The <b>Administrator</b> account is created by default when installing Windows NT on the Server and/or Workstation. The <b>Guest</b> account is disabled by default on the Server, but not on the Workstation. Even though it has been disabled, the account still exists. Therefore, it is recommended that the <b>Administrator</b> account be renamed on servers and workstations. This will minimize the number of known attacks available to a malicious user.</p>	<Site Specific>
<p><b><u>Change Guest Account to</u></b>                      (U) The <b>Guest</b> accounts are created by default when installing Windows NT on the Server and/or Workstation. The <b>Guest</b> account is disabled by default on the Server, but not on the Workstation. Even</p>	<Site Specific>

# UNCLASSIFIED

<b>Security Attribute</b>	<b>Recommended Security Setting</b>
though it has been disabled, the account still exists. Therefore, it is recommended that the <b>Guest</b> accounts be renamed on servers and workstations. This will minimize the number of known attacks available to a malicious user.	
<p><b><u>Clear virtual memory pagefile when system Shuts down</u></b>            (U) Virtual Memory support of Windows NT uses a system page file to swap pages from memory of different processes onto disk when they are not being actively used. On a running system, this page file is opened exclusively by the operating system and hence is well-protected. However, to implement a secure Windows NT environment the system page file should be wiped clean when Windows NT shuts down. This ensures sensitive information that may be in the page file is not available to a malicious user.</p>	Enabled
<b><u>Digitally sign client-side communication always</u></b>	Not Configured
<b><u>Digitally sign client-side communication when possible</u></b>	Not Configured
<b><u>Digitally sign server-side communication always</u></b>	Not Configured
<b><u>Digitally sign server-side communication when possible</u></b>	Not Configured
<p><b><u>Disallow enumeration of account names and shares by anonymous</u></b>            (U) Starting Windows NT 4.0 Service Pack 3 a mechanism for administrators to restrict the ability for anonymous logon users (also known as NULL session connections) to list account names and enumerate share names. Manual step, set the registry key value to enable this feature is:            Hive: HKEY_LOCAL_MACHINE            Key: \System\CurrentControlSet\Control\LSA            Name: RestrictAnonymous            Type: REG_DWORD            Value: 1</p>	Enabled
<p><b><u>Do not disable last name in logon screen</u></b>            (U) By default, Windows NT places the user name of the last user to log on the computer in the User name text box of the <b>Logon</b> dialog box. This makes it more convenient for the most frequent user to log on. To enhance security, prevent Windows NT from displaying the user name from the last logon. This is especially important if a generally accessible computer is being used for system administration.</p>	Enabled
<p><b><u>Forcibly logoff when logon hours expire</u></b>            (U) Disconnects a user account from any servers on the domain when it exceeds its logon hours.</p>	<Site Specific>
<p><b><u>Message text for users attempting to log on</u></b>            (U) It is recommended that systems display a warning message before logon, indicating the private nature of the system. Many organizations use this message box to display a warning message that notifies potential users that their use can be monitored and they can be held legally liable if they attempt to use the computer without having been properly authorized to do so. The absence of such a notice could be construed as an invitation, without restriction, to enter and browse the system.</p>	<see Appendix K for sample>
<p><b><u>Message title for users attempting to log on</u></b>            (U) In conjunction with the Logon Text it recommended that systems display a warning message title before logon, indicating the private nature of the system.</p>	<see Appendix K for sample>
<p><b><u>Number of previous logons to cache in case Domain Controller not available</u></b>            (U) The default Windows NT configuration caches the last logon credentials for users who log on interactively to a system. This</p>	0

<b>Security Attribute</b>	<b>Recommended Security Setting</b>
feature is provided for system availability reasons such as the user's machine is disconnected from the network or domain controllers are not available. Even though the credential cache is well protected, to implement a secure Windows NT environment, this feature should be disabled.	
<p><b><u>Prevent user from installing print drivers</u></b>  (U) Enables the system spooler to restrict adding printer drivers to administrators and print operators (on server) or power users (on workstation).  Manual Step, sets registry key:  \System\CurrentControlSet\Control\Print\Providers\LanMan Print Services to 1, which is used to control who can add printer drivers using the print folder. This key value should be set to 1.</p>	Enabled
<p><b><u>Restrict CDROM access to locally logged on user only</u></b>  (U) By default, Windows NT allows any program to access files on CD-ROM drives. In a highly secure, multi-user environment, only allow interactive users to access these devices. When operating in this mode, the CD-ROM(s) are allocated to a user as part of the interactive logon process. These devices are automatically deallocated when the user logs off.</p>	Enabled
<p><b><u>Restrict Floppy access to locally logged on user only</u></b>  (U) By default, Windows NT allows any program to access files on floppy drives. In a highly secure, multi-user environment, only allow interactive users to access these devices. When operating in this mode, the floppy disks are allocated to a user as part of the interactive logon process. These devices are automatically deallocated when the user logs off.</p>	Enabled
<p><b><u>Restrict management of shares resources such as COM1</u></b>  (U) Restrict the access of shared resources.</p>	Enabled
<p><b><u>Secure Channel: Digitally encrypt or sign secure channel data always</u></b></p>	Not Configured
<p><b><u>Secure Channel: Digitally encrypt or sign secure channel data when possible</u></b></p>	Not Configured
<p><b><u>Secure Channel: Digitally sign secure channel when possible</u></b></p>	Not Configured
<p><b><u>Secure System partition (for RISC platforms only)</u></b></p>	Not Configured
<p><b><u>Send downlevel LanMan compatible password</u></b>  (U) Windows NT supports the following two types of challenge/response authentication:  LanManager (LM) challenge/response, for backwards compatibility  Windows NT challenge/response, for stronger authentication  To allow access to servers that only support LM authentication, Windows NT clients currently send both authentication types. The LM Password Hotfix allows clients to be configured to send only Windows NT authentication. This removes the use of LM challenge/response messages from the network, preventing many attacks.  After applying the hotfix, the following registry key is added:  Hive: HKEY_LOCAL_MACHINE  Key: \System\CurrentControlSet\Control\LSA  Name: LMCompatibilityLevel  Type: REG_DWORD  Value: 0, 1, 2  0 – Send both Windows NT and LM password authentication.  1 – Send Windows NT and LM password authentication only if the server requests it.  2 – Never send LM password authentication.  <b>WARNING: Setting Value = 2 on a Windows NT</b></p>	As Requested

<b>Security Attribute</b>	<b>Recommended Security Setting</b>
<p>system prevents connection to systems that support only LM authentication, such as Windows 95<sup>®</sup> and Windows for Workgroups<sup>®</sup>. This should only be set if running a homogeneous Windows NT network. Doing so provides the strongest level of protection and prevents many common Windows NT attacks.</p>	
<p><b><u>Send unencrypted password in order to connect to 3<sup>rd</sup> Party SMB server</u></b>            (U) Windows NT supports the following two types of challenge/response authentication:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> LanManager (LM) challenge/response, for backwards compatibility</li> <li><input type="checkbox"/> Windows NT challenge/response, for stronger authentication</li> </ul> <p>To allow access to servers that only support LM authentication, Windows NT clients currently send both authentication types. The LM Password Hotfix allows clients to be configured to send only Windows NT authentication. This removes the use of LM challenge/response messages from the network, preventing many attacks.</p>	Disabled
<p><b><u>Shutdown system immediately if unable to log security audits</u></b>            (U) If events cannot be written to the security log, the system should be halted immediately. If the system halts as a result of a full log, an administrator must restart the system and clear the log.            Note: Before clearing the security log, save the data to disk.            Manual Step for Setting and Clearing Crash on Audit Fail            To enable Halt on Audit Failure.            Modify the following Registry key value:            Hive: HKEY_LOCAL_MACHINE            Key: \System\CurrentControlSet\Control\Lsa            Name: CrashOnAuditFail            Type: REG_DWORD            Values: 1 (Crash if the audit log is full.)            2 (This value is set by the operating system just before it crashes due to a full audit log. While the value is 2, only the administrator can log on to the computer. This value confirms the cause of the crash.)</p> <p>To reset, change this value back to 1            Select the  <b>HKEY_LOCAL_MACHINE on Local Machine</b> window            Navigate down the \System\CurrentControlSet\Control path, double clicking on each key along the way            Highlight the Lsa key            Select <b>Add Value...</b> from the <b>Edit</b> menu            Enter <b>“ProtectionMode”</b> for <b>Value Name:</b>            Select <b>REG_DWORD</b> from the <b>Data Type:</b> drop down list            Click <b>OK</b> in the <b>Add Value</b> window            Enter <b>1</b> for the <b>Data:</b> value in the <b>DWORD Editor</b>            Click <b>OK</b> to close the <b>DWORD Editor</b></p>	Enabled

**(U) Table 8 Recommended Security Options Configuration**

(U) **NOTE:** After making any modifications to the configuration files make sure the changes are saved (See Chapter 4) and then test the changes before installing them on an operational network.

**(U) Event Logs**

(U) Windows NT event logs record system events as they occur. The Security, Application, and System event logs contain information generated by the specified audit settings. In order to record, retrieve, and store event logs on a Windows NT system, the administrator must enable auditing and configure the events to be audited as outlined in the Local Policies section earlier in this chapter. In addition to the audit settings enabled in the SCM, auditing of other system objects such as specific files, registry keys, and printers can be enabled. For more details on event logs and auditing, refer to Chapter 7.

**(U) Modifying the Event Log Settings via the Security Configuration Manager**

(U) To view event log settings of an SCM template:

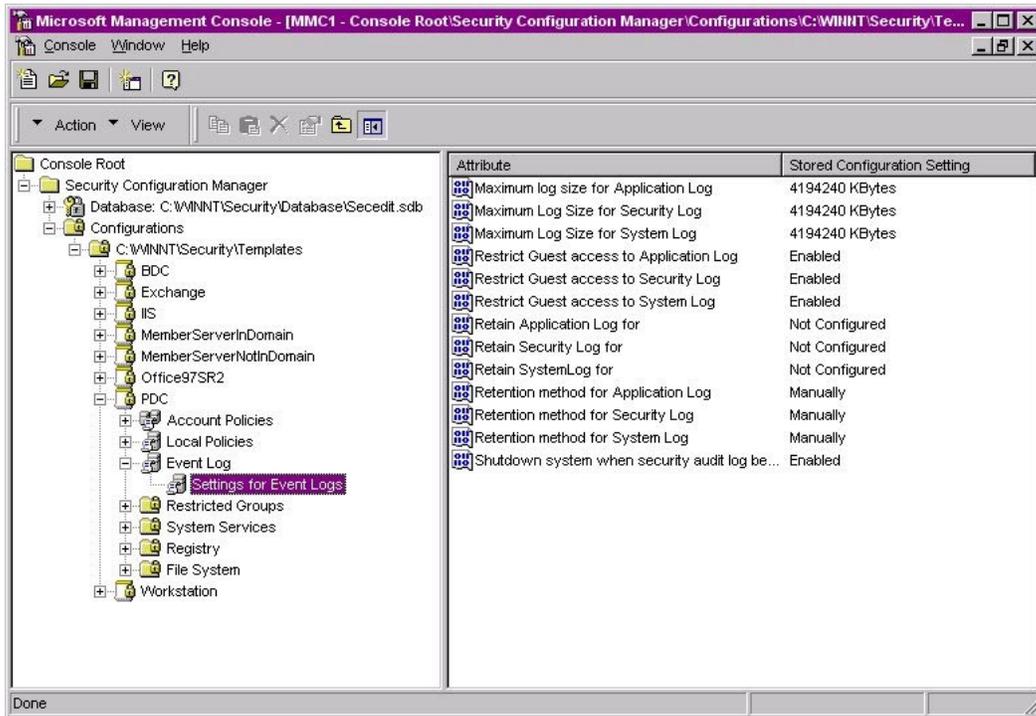
- Double-click on the **Security Configuration Manager** node. This reveals the following folders:
  - Database: Not loaded**
  - Configurations**
- Double click on the **Configurations** node
- Double-click on the default configuration file directory (%SystemRoot%\Security\Templates)
- Double-click on a specific configuration file
- Double-click on **Event Log**
- Double-click on **Settings for Event Logs** (See (U) Figure 9)
- (U) Double-click on each of the settings described below to view or edit the current settings. See (U) Table 9 for recommended event log settings.

(U) **NOTE:** After making any modifications to the configuration files make sure the changes are saved (See Chapter 4) and then test the changes before installing them on an operational network.

<b>Event Log Settings</b>	<b>Recommended Settings</b>
<p><b><u>Maximum Log Size for Application Log</u></b>  <b><u>Maximum Log Size for Security Log</u></b>  <b><u>Maximum Log Size for System Log</u></b></p> <p>(U) If the event logs are too small, logs will fill up often and administrators must save and clear the event logs more frequently than required. Allowable values range from 64 KB to 4194240 KB.  <b>(U) NOTE: This setting will allow the log file to equal the size of the available space on the hard disk or up to 4GB, whichever is smaller. This is to ensure that the system will not halt if the event log exceeds specified log space while there is additional space available on the hard drive.</b></p>	4194240 KBytes
<p><b><u>Restrict Guest access to Application Log</u></b>  <b><u>Restrict Guest access to Security Log</u></b>  <b><u>Restrict Guest access to System Log</u></b></p> <p>(U) Default configuration allows guests and null logons the ability to view event logs (system and application logs). While the security log is protected from guest access by default, it is viewable by users who</p>	Enabled

Event Log Settings	Recommended Settings
<p>have the "Manage Audit Logs" user right. This option disallows guests and null logons from viewing any of the event logs.</p>	
<p><b><u>Retain Application Log for</u></b>  <b><u>Retain Security Log for</u></b>  <b><u>Retain System Log for</u></b>            (U) These options control how long the event logs will be retained before they are overwritten. Since it is not recommended that any event logs be overwritten when they become full, this option should not be configured.</p>	<p>Exclude this setting from configuration</p>
<p><b><u>Retention method for Application Log</u></b>  <b><u>Retention method for Security Log</u></b>  <b><u>Retention method for System Log</u></b>            (U) How the operating system handles event logs that have reached their maximum size. The event logs can be overwritten after a certain number of days, overwritten when they become full, or have to be cleared manually. To ensure that no important data is lost, especially in the event of a security breach of the system, the event logs should not be overwritten.</p>	<p>Do not overwrite events (clean log manually)</p>
<p><b><u>Shutdown system when security audit log becomes full</u></b>            (U) If events cannot be written to the security log, the system should be halted immediately. If the system halts as a result of a full log, an administrator must restart the system and clear the log.</p>	<p>Enable</p>

(U) Table 9 Recommended Event Log Settings



(U) Figure 9 Event Log Recommended Configuration

**(U) Managing the Event Logs****(U) Saving And Clearing the Audit Logs**

- Select **Start** → **Programs** → **Administrative Tools (Common)** → **Event Viewer**
- Select the appropriate event log from the **Log Menu**
- Select **Clear All Events** from the **Log** menu
- Click **Yes** to save settings
- Enter a unique file name
- Click the **Save** button
- Click **Yes** to clear the event log
- Repeat the above steps for each log

**(U) Resetting the Audit Log Settings After the System Halts**

(U) If the system halts as a result of a full log, an administrator must restart the system and clear the log.

**(U) NOTE:** Before clearing the security log, save the data to disk.

(U) Use the Registry Editor to modify the following Registry key value:

Hive: **HKEY\_LOCAL\_MACHINE**  
 Key: **\System\CurrentControlSet\Control\Lsa**  
 Name: **CrashOnAuditFail**  
 Type: **REG\_DWORD**  
 Value: **1**

- Log on as an administrator
- Select **Start** → **Run...**
- Type Regedt32.exe in the **Open** dialog box
- Navigate down the **\System\CurrentControlSet\Control\Lsa** path, double clicking on each key along the way
- Double click the **CrashOnAuditFail** key
- Enter **1** in the DWORD editor

**(U) NOTE:** This value is set by the operating system just before it crashes due to a full audit log. While the value is 2, only the administrator can log on to the computer. This value confirms the cause of the crash. Reset the value 1

- Click **OK** to continue
- Exit the registry editor

## (U) Restricted Groups

(U) The Restricted Groups option allows the administrator to manage the membership of sensitive groups. These groups can either be local (e.g. Administrators, Power Users, Server Operators, etc.) or global (e.g. Domain Admins, Domain Users, etc.), built-in or created. For example, if you want the Administrators group to only consist of the built-in Administrator account, you could add the Administrators group to the Restricted Groups option and add Administrator in the **Members of Administrators** column. This setting could prevent other users from elevating their privilege to the Administrators group through various attack tools and hacks.

(U) Not all groups need to be added to the Restricted Group list. It is recommended that only sensitive groups be configured through the SCM. Any groups not listed will retain their membership lists.

(U) For all groups listed for this option, any groups and/or users listed which are not currently members of that group are added, and any users and/or groups currently members of the group but not listed in the configuration file are removed.

### (U) Modifying Restricted Groups via the Security Configuration Manager

(U) Since the settings in the **Restricted Groups** option should be site-specific, no restricted group settings are configured in the companion configuration (*inf*) files. However, you may wish to restrict the membership of sensitive groups within the domain.

(U) To view restricted group settings of an SCM template:

- Double-click on the Security Configuration Manager node. This reveals the following folders:
  - **Database: Not loaded**
  - **Configurations**
- Double click on the **Configurations** node
- Double-click on the default configuration file directory (%SystemRoot%\Security\Templates)
- Double-click on a specific configuration file
- Double-click on **Restricted Groups**

(U) The following steps describe how to add a restricted group to the list.

- Right-click on **Restricted Groups**
- Choose **Add Group** from the pull-down menu
- Double-click on each group you wish to add
- Click **OK**
- The new group(s) you added will now appear in the right frame.
- Double click on a newly added group
- In the **Members of** column, click on the **Add** button.
- Double-click on each group and/or user you wish to be members of the group.

- Click **OK**

**WARNING:** If you add a Restricted Group and then delete it from the configuration file at a later time, you must ensure that the group is indeed gone from the inf file. Windows 2000 will allow for control over reverse membership as part of the is a Member of column. This column lists groups to which the restricted group can belong. This option is not yet available with Windows NT 4.0 and is grayed out in the GUI. However, entries for Member\_Of still exist in the inf file. Despite deleting the groups through the GUI, the Member\_Of section may not be deleted from the actual inf. You must manually open the inf file in a text editor and remove all entries under the Group Management section. Failure to do so may result in unpredictable behavior regarding group membership.

(U) **NOTE:** After making any modifications to the configuration files make sure the changes are saved (See Chapter 4) and then test the changes before installing them on an operational network.

## (U) Services

(U) The **System Services** option allows for configuration of network, file, and print services. Configuration options include service startup settings (Automatic, Manual, or Disabled). Security settings can also be established that govern which users and/or groups can read and execute, write to, delete, start, pause, or stop a service.

### (U) Modifying System Services via the Security Configuration Manager

(U) Because of the broad nature of this area, system service configuration is site-specific. Services not listed in this option can be added. However, you will need to create and attach a new SCM DLL attachment. For more information on creating SCM attachments, refer to Microsoft's Technet January, 1999 white paper "*MS Security Configuration Manager for Windows NT 4.*"

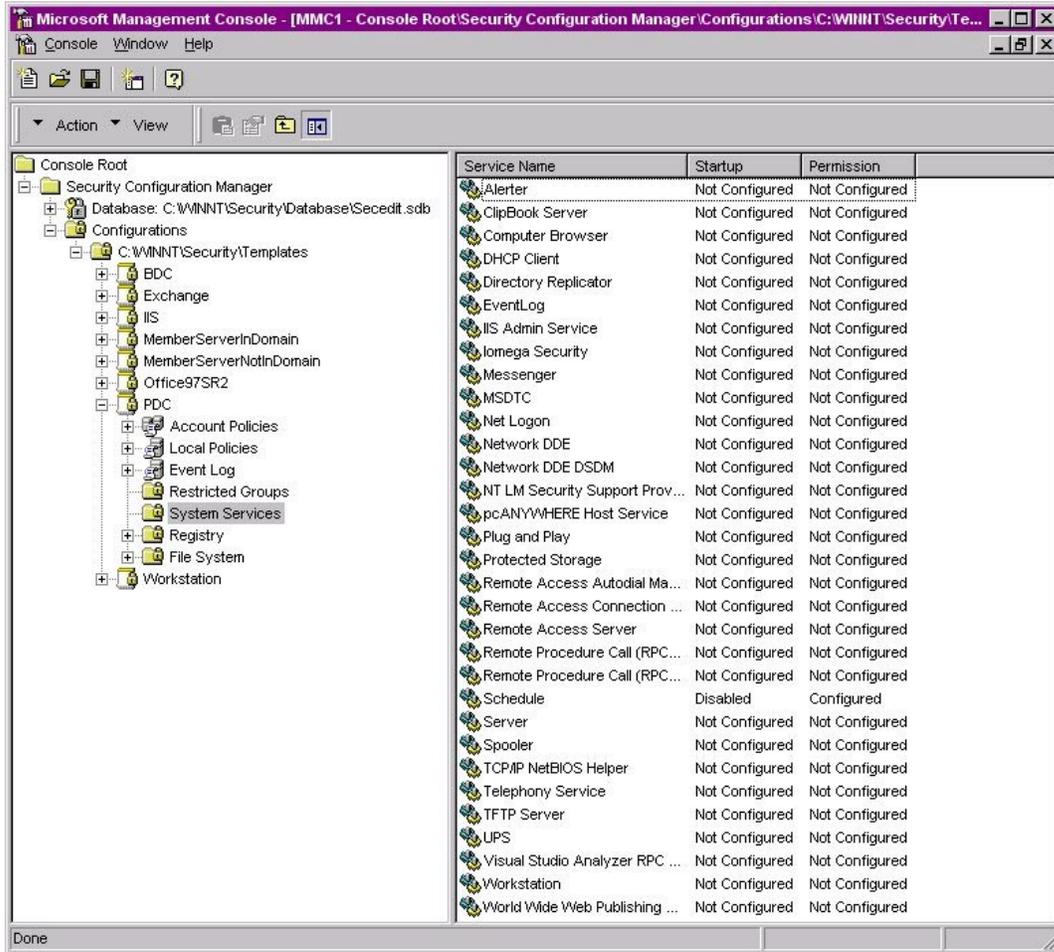
(U) To view system service settings of an SCM template:

- Double-click on the **Security Configuration Manager** node. This reveals the following folders:
  - **Database: Not loaded**
  - **Configurations**
    - Double click on the **Configurations** node
    - Double-click on the default configuration file directory (%SystemRoot%\Security\Templates)
    - Double-click on a specific configuration file
    - Double-click on **System Services** (See (U) Figure 10)

(U) The following steps describe how to configure system service settings.

- Double-click on the service to configure
- Uncheck the **Exclude this setting from configuration** checkbox
- Select the **Service startup mode:** **Automatic**, **Manual**, or **Disabled**

- Click **Edit Security**
- Click **Add** to add groups and/or users to the access list.
  - Double-click on each user or group to add.
  - Click **OK**
  - Check the permissions that each user or group should have for that service
- Click **Remove** to remove groups and/or users from the access list.



**(U) Figure 10 System Services Recommended Settings**

The only service configured in the accompanying configuration (*inf*) file is the Schedule service (See (U) Figure 10). The Schedule service allows administrators the ability to remotely execute applications on domain systems. However, by having the schedule service active, the potential exists for an unauthorized user to gain access to the domain by inserting a malicious program into the schedule task list.

It is recommended that the Schedule service be disabled. When necessary, the service may be started and then disabled once it is no longer needed. Also, the following permissions should be set on the service:

- Administrators: (configure through Advanced tab) Query Configuration, Query Status, Enumerate dependents, Stop, Interrogate, Read permissions

- System: Read, Start, Stop, and Pause
  - (U) **NOTE:** After making any modifications to the configuration files make sure the changes are saved (See Chapter 4) and then test the changes before installing them on an operational network.

## (U) Registry

(U) In order to implement adequate security in a Windows NT environment, registry keys and their associated permissions must be changed.

(U) **WARNING:** By default, some protections are set on the various components of the registry that allow work to be done while providing standard-level security. For high-level security, additional access rights must be added to specific registry keys. This should be done with caution because programs that users need to do their jobs often require access to certain keys on the users' behalf. Care should be taken to follow these steps exactly, as additional, unnecessary changes to the registry can render a system unusable and even unrecoverable.

### (U) Modifying Registry settings via the Security Configuration Manager

(U) Recommended changes to the registry are listed below. The necessary changes can be made in one of two ways. The first is to use the Security Configuration Manager according to the recommendations found in this chapter. The alternative and more time-consuming method would be to change permissions on each registry key manually.

(U) There are several registry modifications that must be performed manually after the SCM is run. See Chapter 7 for these changes.

(U) To view registry settings of an SCM template:

- Double-click on the **Security Configuration Manager** node. This reveals the following folders:
  - **Database: Not loaded**
  - **Configurations**
- Double click on the **Configurations** node
- Double-click on the default configuration file directory (`%SystemRoot%\Security\Templates`)
- Double-click on a specific configuration file
- Double-click on **Registry**

### (U) Modifying Permissions on a Registry Key

(U) To modify the security settings on a particular registry key already specified in the `inf` file:

- In the right frame, double-click on the key to be changed
- Ensure that the **Overwrite** radio button is selected
- Click **Edit Security**

## UNCLASSIFIED

- Uncheck the **Allow inheritable permissions from parent to propagate to this object** checkbox.
- If the inheritable permissions checkbox was previously checked, click on the **Remove** button in the **Security** dialog box.
- Add/remove users and groups to reflect the recommended permissions.
- For each user and/or group, set the permissions by clicking on the permission checkboxes.
- If the key permissions should encompass the key itself and all subkeys below the key:
  - Click the **Apply** button
  - Click **OK**. Stop here.
- Otherwise, click the **Advanced** button.

**(U) NOTE:** If special access is desired for a user and/or group, this can be configured through the **Advanced** dialog box.

- Double-click on a user and/or group. A **Permission Entry** dialog box will appear.
- In the **Apply** onto pull-down menu, select the correct configuration (e.g. **This key only**).
- Click **OK** to exit the **Permission Entry** dialog box.
- Click **Apply** in the **Advanced** dialog box.
- Click **OK** in the **Advanced** dialog box.
- Click **OK** in the **Properties** dialog box.

### **(U) Adding registry keys to the security configuration**

To add a registry key to the security configuration:

- Right-click on **Registry**
- Select **Add Key** from the pull-down menu
- Select the registry key to be added
- Click **OK**
- A **Configuration Security** dialog box will appear.
- Click **OK**
- Double-click on the registry key in the right frame when it appears
- Configure the permissions according to the steps detailed in the previous **Modifying permissions on a registry key** section.

### **(U) Excluding registry keys from the security configuration**

(U) There are occasions where a specific registry key should retain its current security settings. To ensure that parent keys don't propagate their new permissions down to such registry keys, you may exclude the object from configuration.

(U) To exclude an object:

# UNCLASSIFIED

- In the right frame of **Registry**, double-click on the key to be changed
- Click the **Ignore** radio button.
- Click **OK**

## **(U) Recommended Registry Key Permissions**

(U) Registry keys not explicitly listed below are assumed to inherit the permissions of their parent key. Keys with “Ignore” are explicitly excluded from SCM configuration and retain their original permissions.

(U) The following notation is used in this section:

- \MACHINE – HKEY\_LOCAL\_MACHINE hive
- \CLASSES\_ROOT – HKEY\_CLASSES\_ROOT hive
- \USERS – HKEY\_USERS hive

<b>REGISTRY KEY</b>	<b>USER GROUPS</b>	<b>RECOMMENDED PERMISSIONS</b>
<p><b><u>CLASSES_ROOT</u></b> <i>key and subkeys</i></p> <p>(U) Alias to MACHINE\SOFTWARE\Classes. Contains file associations and COM (Common Object Model) associations.</p>	Administrators Authenticated Users CREATOR OWNER SYSTEM	Full Control Read, Write, Execute Full Control Full Control
<p><b><u>CLASSES_ROOT\hlp</u></b> <i>key</i></p> <p>(U) Help file association.</p>	Administrators Authenticated Users SYSTEM	Full Control Read, Execute Full Control
<p><b><u>CLASSES_ROOT\helpfile</u></b> <i>key and subkeys</i></p> <p>(U) Help file related key.</p>	Administrators Authenticated Users SYSTEM	Full Control Read, Execute Full Control
<p><b><u>MACHINE\HARDWARE</u></b> <i>key and subkeys</i></p> <p>(U) Contains data about the physical configuration of the machine.</p>	Administrators Authenticated Users CREATOR OWNER SYSTEM	Full Control Read, Write, Execute Full Control Full Control
<p><b><u>MACHINE\SOFTWARE</u></b> <i>key and subkeys</i></p> <p>(U) Contains information about the software installed on the local system.</p>	Administrators Authenticated Users CREATOR OWNER SYSTEM	Full Control Read, Write, Execute, Delete Full Control Full Control
<p><b><u>MACHINE\SOFTWARE\Classes</u></b> <i>key and subkeys</i></p> <p>(U) Contains file associations and COM (Common Object Model) associations.</p>	Ignore	
<p><b><u>MACHINE\SOFTWARE\Microsoft\Cryptography</u></b> <i>keys and subkeys</i></p> <p>(U) Contains management for CryptoAPI.</p>	Administrators Authenticated Users SYSTEM	Full Control Read, Execute Full Control

# UNCLASSIFIED

<b>REGISTRY KEY</b>	<b>USER GROUPS</b>	<b>RECOMMENDED PERMISSIONS</b>
<p><b><u>MACHINE\SOFTWARE\Microsoft\NetDDE</u></b> <i>keys and subkeys</i></p> <p>(U) Settings for Network Dynamic Data Exchange, which is a protocol that allows applications to exchange data.</p>	Administrators SYSTEM	Full Control Full Control
<p><b><u>MACHINE\SOFTWARE\Microsoft\Ole</u></b> <i>key and subkeys</i></p> <p>(U) Contains configuration for OLE (Object Linking and Embedding).</p>	Administrators Authenticated Users CREATOR OWNER SYSTEM	Full Control Read, Execute Full Control Full Control
<p><b><u>MACHINE\SOFTWARE\Microsoft\OS/2 Subsystem for NT</u></b> <i>key and subkeys</i></p> <p>(U) Contains support for OS/2 standards. Even if this key is removed, it will reappear at next boot up.</p>	Administrators Authenticated Users CREATOR OWNER SYSTEM	Full Control Read, Execute Full Control Full Control
<p><b><u>MACHINE\SOFTWARE\Microsoft\Protected Storage System Provider</u></b> <i>key and subkeys</i></p> <p>(U) Used to protect user data. Inaccessible.</p>	Ignore	
<p><b><u>MACHINE\SOFTWARE\Microsoft\Rpc</u></b> <i>key and subkeys</i></p> <p>(U) Contains configuration for Remote Procedure Call (RPC).</p>	Administrators Authenticated Users SYSTEM	Full Control Read, Execute Full Control
<p><b><u>MACHINE\SOFTWARE\Microsoft\Secure</u></b> <i>key and subkeys</i></p> <p>(U) Microsoft application configuration data that should be changed only by an administrator.</p>	Administrators Authenticated Users CREATOR OWNER SYSTEM	Full Control Read, Execute Full Control Full Control
<p><b><u>MACHINE\SOFTWARE\Microsoft\Windows</u></b> <i>key and subkeys</i></p> <p>(U) Parameters used by the Win32 subsystem.</p>	Administrators Authenticated Users CREATOR OWNER SYSTEM	Full Control Read, Write, Execute Full Control Full Control
<p><b><u>MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run</u></b> <i>key and subkeys</i></p> <p>(U) Contains names of executables to be run each time the system is started.</p>	Administrators Authenticated Users SYSTEM	Full Control Read, Execute Full Control
<p><b><u>MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce</u></b> <i>key and subkeys</i></p> <p>(U) Contains the name of a program to be executed the first time a user ever logs on.</p>	Administrators Authenticated Users SYSTEM	Full Control Read, Execute Full Control

UNCLASSIFIED

<b>REGISTRY KEY</b>	<b>USER GROUPS</b>	<b>RECOMMENDED PERMISSIONS</b>
<p><u><b>MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx</b></u> <i>key and subkeys</i></p> <p>(U) Contains setup information for some system components and Internet Explorer. Works much the same way as the RunOnce key.</p>	Administrators Authenticated Users SYSTEM	Full Control Read, Execute Full Control
<p><u><b>MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Shell Extensions</b></u> <i>key and subkeys</i></p> <p>(U) Contains all shell extension settings, which are used to extend and expand the Windows NT interface.</p>	Administrators Authenticated Users CREATOR OWNER SYSTEM	Full Control Read, Execute Full Control Full Control
<p><u><b>MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall</b></u> <i>key and subkeys</i></p> <p>(U) Contains uninstall strings for all applications that can be removed in the Add/Remove Programs applet.</p>	Administrators Authenticated Users CREATOR OWNER SYSTEM	Full Control Read, Execute Full Control Full Control
<p><u><b>MACHINE\SOFTWARE\Microsoft\Windows NT</b></u> <i>key and subkeys</i></p> <p>(U) Parameters used by the Windows NT operating system.</p>	Administrators Authenticated Users CREATOR OWNER SYSTEM	Full Control Read, Execute Full Control Full Control
<p><u><b>MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AEDebug</b></u> <i>key and subkeys</i></p> <p>(U) Settings for application debugger (most commonly Dr. Watson).</p>	Administrators Authenticated Users SYSTEM	Full Control Read, Execute Full Control
<p><u><b>MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Compatibility</b></u> <i>key and subkeys</i></p> <p>(U) Contains data for legacy applications not completely compatible with Windows NT.</p>	Administrators Authenticated Users CREATOR OWNER SYSTEM	Full Control Read, Write, Execute Full Control Full Control
<p><u><b>MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Font Drivers</b></u> <i>key and subkeys</i></p> <p>(U) Contains drivers used to display fonts.</p>	Administrators Authenticated Users SYSTEM	Full Control Read, Execute Full Control
<p><u><b>MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Font Mapper</b></u> <i>key and subkeys</i></p> <p>(U) Contains settings for mappings of unavailable fonts to existing fonts.</p>	Administrators Authenticated Users SYSTEM	Full Control Read, Execute Full Control
<p><u><b>MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options</b></u> <i>key and subkeys</i></p> <p>(U) Parameters for viewing images.</p>	Administrators Authenticated Users SYSTEM	Full Control Read, Execute Full Control

UNCLASSIFIED

<b>REGISTRY KEY</b>	<b>USER GROUPS</b>	<b>RECOMMENDED PERMISSIONS</b>
<p><b><u>MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\IniFileMapping</u></b>  <i>key and subkeys</i></p> <p>(U) Registry mappings of 16-bit Windows applications' initialization files.</p>	Administrators Authenticated Users SYSTEM	Full Control Read, Execute Full Control
<p><b><u>MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib</u></b>  <i>key and subkeys</i></p> <p>(U) Parameters for the Performance Library, which collects information for Performance Monitor.</p>	Administrators Authenticated Users SYSTEM	Full Control Read, Execute Full Control
<p><b><u>MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\009</u></b>  <i>key and subkeys</i></p> <p>(U) Contains performance names and descriptions.</p>	Ignore	
<p><b><u>MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones</u></b>  <i>key and subkeys</i></p> <p>(U) Time zone settings.</p>	Administrators Authenticated Users SYSTEM	Full Control Read, Execute Full Control
<p><b><u>MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon</u></b>  <i>key and subkeys</i></p> <p>(U) Controls logon sequence for starting Windows NT.</p>	Administrators Authenticated Users SYSTEM	Full Control Read, Execute Full Control
<p><b><u>MACHINE\SOFTWARE\Program Groups</u></b>  <i>key and subkeys</i></p> <p>(U) Indicates whether all former program groups from a pre-NT 4.0 OS on the system have been converted to the new NT 4.0 directory structure. Subkeys only present if a previous NT version was on the system.</p>	Administrators Authenticated Users CREATOR OWNER SYSTEM	Full Control Read, Execute Full Control Full Control
<p><b><u>MACHINE\SOFTWARE\Secure</u></b>  <i>key and subkeys</i></p> <p>(U) Application configuration data that should be changed only by an administrator.</p>	Administrators Authenticated Users CREATOR OWNER SYSTEM	Full Control Read, Execute Full Control Full Control
<p><b><u>MACHINE\SOFTWARE\Windows 3.1 Migration Status</u></b>  <i>key and subkeys</i></p> <p>(U) Contains data if system has been upgraded from Windows 3.x to Windows NT. Indicates whether upgradable parameters have been successfully migrated.</p>	Administrators Authenticated Users CREATOR OWNER SYSTEM	Full Control Read, Execute Full Control Full Control

UNCLASSIFIED

<b>REGISTRY KEY</b>	<b>USER GROUPS</b>	<b>RECOMMENDED PERMISSIONS</b>
<p><u><b>MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg</b></u> <i>key and subkeys</i></p> <p>(U) The security permissions set on this key define which users or groups can connect to the system for remote registry access. The default Windows NT Workstation installation does not define this key and does not restrict remote access to the registry. Windows NT Server permits only administrators remote access to most of the registry. It is highly recommended that only administrators have remote access to the registry.</p>	Administrators SYSTEM	Full Control Full Control
<p><u><b>MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Shares</b></u> <i>key and subkeys</i></p> <p>(U) Contains settings for shares on the local system.</p>	Administrators Authenticated Users CREATOR OWNER SYSTEM	Full Control Read, Execute Full Control Full Control
<p><u><b>MACHINE\SYSTEM\CurrentControlSet\Services\Schedule</b></u> <i>key and subkeys</i></p> <p>(U) Contains settings for the schedule service.</p>	Administrators Authenticated Users CREATOR OWNER SYSTEM	Full Control Read, Execute Full Control Full Control
<p><u><b>MACHINE\SYSTEM\CurrentControlSet\Services\UPS</b></u> <i>key and subkeys</i></p> <p>(U) Contains information on the Uninterruptible Power Supply if it is installed.</p>	Administrators Authenticated Users CREATOR OWNER SYSTEM	Full Control Read, Execute Full Control Full Control
<p><b>USERS\DEFAULT</b> <i>key and subkeys</i></p> <p>(U) Profile that is used while the Windows NT CTRL+ALT+DEL logon message is displayed.</p>	Administrators Authenticated Users SYSTEM	Full Control Read, Execute Full Control
<p><u><b>USERS\DEFAULT\Software\Microsoft\NetDDE</b></u> <i>key and subkeys</i></p> <p>(U) Settings for Network Dynamic Data Exchange, which is a protocol that allows applications to exchange data.</p>	Administrators SYSTEM	Full Control Full Control
<p><u><b>USERS\DEFAULT\Software\Microsoft\Protected Storage Systems Provider</b></u> <i>key and subkeys</i></p> <p>(U) Used to protect user data. Inaccessible.</p>	Ignore	
<p><u><b>USERS\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Policies</b></u> <i>key and subkeys</i></p> <p>(U) Used to manage RASC (Recreational Software Advisory Council) ratings.</p>	Administrators Authenticated Users CREATOR OWNER SYSTEM	Full Control Read, Execute Full Control Full Control

**(U) Table 10 Recommended Registry Settings**

(U) NOTE: After making any modifications to the configuration files make sure the changes are saved (See

Chapter 4) and then test the changes before installing them on an operational network.

## (U) File System

### (U) NTFS Overview

(U) NTFS is a highly secure file system that provides a reliable way to safeguard valuable information. NTFS works in concert with the Windows NT user account system to allow authenticated users access to files. The system provides extended permissions for controlling access to files and prohibits easy access to data on disk if someone manages to boot the system with another operating system. **To implement the highest level of security, always format Windows NT partitions with the NT File System.**

(U) It is important to understand that Windows NT does not encrypt data or system files stored on a physical disk. Since file data is not encrypted, an intruder gaining physical access to any of the NTFS formatted volumes can use a low-level, byte-editing program to read or change information on those volumes. The security provided by NTFS is based on system controls that are managed by the Windows NT operating system. As long as Windows NT is operating, NTFS permissions and user access control lists prevent unauthorized users from accessing files either locally or over the network.

(U) With NTFS, Windows NT allows for varying levels of file access permissions to users or groups of users. Coupled with file access permissions is the concept of “inheritance.” By default, newly created files or folders inherit the parent folder’s file access permissions.

### (U) Modifying File System settings via the Security Configuration Manager

(U) The recommended changes to system files and folders are listed in (U) Table 11.

(U) The necessary changes can be made in one of two ways. The first method is to use the Security Configuration Manager and the provided template to apply the recommended file and folder permissions. The alternative and more time-consuming method is to change permissions on each file and folder manually.

(U) There are several file system changes that must be manually completed after running the SCM. See Chapter 7 for the additional modifications.

(U) To view file system settings of an SCM template:

- Double-click on the **Security Configuration Manager** node. This reveals the following folders:
  - **Database: Not loaded**
  - **Configurations**
- Double click on the **Configurations** node
- Double-click on the default configuration file directory (%SystemRoot%\Security\Templates)
- Double-click on a specific configuration file
- Double-click on **File System**

**(U) Modifying Permissions on a File or Folder**

(U) To modify the security settings on a particular file or folder already specified in the `inf` file:

- In the right frame, double-click on the file or folder to be changed
- Ensure that the **Overwrite** radio button is selected
- Click **Edit Security**
- Uncheck the **Allow inheritable permissions from parent to propagate to this object** checkbox.
- If the inheritable permissions checkbox was previously checked, click on the **Remove** button in the **Security** dialog box.
- Add/remove users and groups to reflect the recommended permissions.
- For each user and/or group, set the permissions by clicking on the permission checkboxes.
- If the folder permissions should encompass the folder itself, all files within the folder, and all subfolders:
  - Click the **Apply** button
  - Click **OK**. Stop here.
- Otherwise, click the **Advanced** button.
- Double-click on a user and/or group. A **Permission Entry** dialog box will appear.
- In the **Apply** onto pull-down menu, select the correct configuration (e.g. **This folder only**).
- Click **OK** to exit the **Permission Entry** dialog box.
- Click **Apply** in the **Advanced** dialog box.
- Click **OK** in the **Advanced** dialog box.
- Click **OK** in the **Properties** dialog box.

**(U) Adding files or folders to the security configuration**

(U) To add a file or folder to the security configuration:

- Right-click on **File System**
- Select **Add Files** or **Add Folder** from the pull-down menu
- Select the file or folder to be added
- Click **OK**
- A **Configuration Security** dialog box will appear.
- Configure the permissions according to the steps detailed in the previous **Modifying permissions on a file or folder** section.

**(U) Excluding files or folders from the security configuration**

(U) There are occasions where a specific file or folder should retain its current security settings. To ensure that parent folders don't propagate their new permissions down to such files or folders, you may exclude the object from configuration.

(U) To exclude an object:

- In the right frame of **File System**, double-click on the file or folder to be changed
- Click the **Ignore** radio button.
- Click **OK**

**(U) Recommended File and Folder Permissions**

(U) Folders and files not explicitly listed below are assumed to inherit the permissions of their parent folder. Folders with "Ignore" are explicitly excluded from SCM configuration and retain their original permissions.

(U) Folders and files in the table below are alphabetized as they appear in the SCM GUI.

(U) The following system variables are referenced in the file permissions within the SCM configuration file:

- **%SystemDrive%** - The drive letter on which Windows NT is installed. This is usually C:\.
- **%SystemRoot%** - The folder containing the Windows NT operating system files. This is usually %SystemDrive%\winnt.
- **%SystemDirectory%** - %SystemRoot%\system32

**Special Consideration for an IIS Server**

Add the following permissions on the %SystemDrive%\InetPub\wwwroot, %SystemDrive%\InetPub\ftproot, and %SystemDrive%\InetPub\scripts folders:

Administrators	Full Control
Authenticated Users	Read, Execute
CREATOR OWNER	Full Control
INTERACTIVE	Read, Execute
IUSR_<computer_name>	Read, Execute
IWAM_<computer_name>	Read, Execute
SYSTEM	Full Control

# UNCLASSIFIED

(U) NOTE: Shaded entries in the table indicate application-specific folders or files. These files may or may not exist on your system.

<b>FOLDER OR FILE</b>	<b>USER GROUPS</b>	<b>RECOMMENDED PERMISSIONS</b>
<p><b><u>%SystemDirectory%</u></b> <i>folder, subfolders, and files</i></p> <p>(U) Contains many operating system DLLs, drivers, and executable programs.</p>	Administrators Authenticated Users CREATOR OWNER SYSTEM	Full Control Read, Execute Full Control Full Control
<p><b><u>%SystemDirectory%\config</u></b> <i>folder, subfolders, and files</i></p> <p>(U) Contains registry hive files.</p>	Administrators SYSTEM	Full Control Full Control
<p><b><u>%SystemDirectory%\Ntbackup.exe</u></b> <i>file</i></p> <p>(U) File system backup program.</p>	Administrators SYSTEM	Full Control Full Control
<p><b><u>%SystemDirectory%\rcp.exe</u></b> <i>file</i></p> <p>(U) Program used to execute remote procedure calls.</p>	Administrators SYSTEM	Full Control Full Control
<p><b><u>%SystemDirectory%\Rdisk.exe</u></b> <i>file</i></p> <p>(U) Program used to create an Emergency Repair Disk.</p>	Administrators SYSTEM	Full Control Full Control
<p><b><u>%SystemDirectory%\Regedt32.exe</u></b> <b><u>%SystemDirectory%\Regedt32.cnt</u></b> <b><u>%SystemDirectory%\Regedt32.hlp</u></b> <i>file</i></p> <p>(U) Registry editing tool and associated help files.</p>	Administrators SYSTEM	Full Control Full Control
<p><b><u>%SystemDirectory%\replxport</u></b> <i>folder, subfolders, and files</i></p> <p>(U) Folder containing scripts and files to be replicated to other replication servers.</p>	Administrators Authenticated Users CREATOR OWNER Replicator SYSTEM	Full Control Read, Execute Full Control Read, Execute Full Control
<p><b><u>%SystemDirectory%\replimport</u></b> <i>folder, subfolders, and files</i></p> <p>(U) Folder containing scripts and files that have been replicated from other replication servers.</p>	Administrators Authenticated Users CREATOR OWNER Replicator SYSTEM	Full Control Read, Execute Full Control Modify Full Control
<p><b><u>%SystemDirectory%\rexec.exe</u></b> <i>file</i></p> <p>(U) Program used to execute remote calls.</p>	Administrators SYSTEM	Full Control Full Control
<p><b><u>%SystemDirectory%\rsh.exe</u></b> <i>file</i></p> <p>(U) Program used to execute a remote shell.</p>	Administrators SYSTEM	Full Control Full Control
<p><b><u>%SystemDirectory%\spool\Printers</u></b> <i>folder, subfolders, and files</i></p> <p>(U) Printer spool.</p>	Administrators Authenticated Users CREATOR OWNER Replicator SYSTEM	Full Control Modify Full Control Modify Full Control

UNCLASSIFIED

<b>FOLDER OR FILE</b>	<b>USER GROUPS</b>	<b>RECOMMENDED PERMISSIONS</b>
<p><b><u>%SystemDrive%</u></b>  <i>folder, subfolders, and files</i></p> <p>(U) Drive on which Windows NT is installed. Contains important system startup and configuration files.</p>	Administrators Authenticated Users CREATOR OWNER SYSTEM	Full Control Read, Write, Execute Full Control Full Control
<p><b><u>%SystemDrive%\autoexec.bat</u></b>  <b><u>c:\autoexec.bat</u></b>  <i>file</i></p> <p>(U) Initialization file for DOS applications.</p>	Administrators Authenticated Users SYSTEM	Full Control Read, Execute Full Control
<p><b><u>%SystemDrive%\boot.ini</u></b>  <b><u>c:\boot.ini</u></b>  <i>file</i></p> <p>(U) Boot menu.</p>	Administrators SYSTEM	Full Control Full Control
<p><b><u>%SystemDrive%\config.sys</u></b>  <b><u>c:\config.sys</u></b>  <i>file</i></p> <p>(U) Initialization file for DOS applications.</p>	Administrators Authenticated Users SYSTEM	Full Control Read, Execute Full Control
<p><b><u>%SystemDrive%\io.sys</u></b>  <i>file</i></p> <p>(U) Initialization file for DOS applications.</p>	Administrators Authenticated Users SYSTEM	Full Control Read, Execute Full Control
<p><b><u>%SystemDrive%\msdos.sys</u></b>  <i>file</i></p> <p>(U) Initialization file for DOS applications.</p>	Administrators Authenticated Users SYSTEM	Full Control Read, Execute Full Control
<p><b><u>%SystemDrive%\ntdetect.com</u></b>  <b><u>c:\ntdetect.com</u></b>  <i>file</i></p> <p>(U) Hardware detector during Windows NT boot.</p>	Administrators SYSTEM	Full Control Full Control
<p><b><u>%SystemDrive%\ntldr</u></b>  <b><u>c:\ntldr</u></b>  <i>file</i></p> <p>(U) Windows NT operating system loader.</p>	Administrators SYSTEM	Full Control Full Control
<p><b><u>%SystemDrive%\NTReskit</u></b>  <i>folder, subfolders, and files</i></p> <p>(U) Only exists if Windows NT Resource Kit has been installed. Contains resource kit files.</p>	Administrators Authenticated Users CREATOR OWNER SYSTEM	Full Control Read, Execute Full Control Full Control
<p><b><u>%SystemDrive%\pagefile.sys</u></b>  <i>file</i></p> <p>System pagefile. Cannot be accessed since it is being used.</p>	Ignore	
<p><b><u>%SystemDrive%\Program Files</u></b>  <i>folder, subfolders, and files</i></p> <p>(U) Default folder for installed applications.</p>	Administrators Authenticated Users CREATOR OWNER SYSTEM	Full Control Read, Write, Execute Full Control Full Control

UNCLASSIFIED

<b>FOLDER OR FILE</b>	<b>USER GROUPS</b>	<b>RECOMMENDED PERMISSIONS</b>
<p><b><u>%SystemDrive%\Users</u></b> <i>folder, subfolders, and files</i></p> <p>(U) If folder exists (from a previous NT version), leave permissions intact.</p>	Ignore	
<p><b><u>%SystemDrive%\Win32app</u></b> <i>folder, subfolders, and files</i></p> <p>(U) If folder exists (from a previous NT version), leave permissions intact.</p>	Ignore	
<p><b><u>%SystemRoot%</u></b> <i>folder only</i></p> <p>(U) Folder in which the Windows NT operating system is installed. By default, this is called winnt.</p>	Administrators Authenticated Users CREATOR OWNER SYSTEM	Full Control Read, Write, Execute Full Control Full Control
<p><b><u>%SystemRoot%</u></b> <i>subfolders and files</i></p>	Administrators Authenticated Users CREATOR OWNER SYSTEM	Full Control Read, Execute Full Control Full Control
<p><b><u>%SystemRoot%\\$NtServicePackUninstall\$</u></b> <i>folder, subfolders, and files</i></p> <p>(U) Contains older versions of system files necessary to back off a service pack.</p>	Administrators SYSTEM	Full Control Full Control
<p><b><u>%SystemRoot%\Cookies</u></b> <i>folder, subfolders, and files</i></p> <p>(U) Folder in which cookies generated in web browsing are kept.</p>	Administrators Authenticated Users CREATOR OWNER SYSTEM	Full Control Read, Write, Execute Full Control Full Control
<p><b><u>%SystemRoot%\drwtsn32.log</u></b> <i>file</i></p> <p>(U) Dr. Watson application error log file.</p>	Administrators Authenticated Users CREATOR OWNER SYSTEM	Full Control Modify Full Control Full Control
<p><b><u>%SystemRoot%\Help</u></b> <i>folder, subfolders, and files</i></p> <p>(U) System Help files. In order for authenticated users to use the full capabilities of help, they must be able to add index files to this folder</p>	Administrators Authenticated Users CREATOR OWNER SYSTEM	Full Control Read, Write, Execute Full Control Full Control
<p><b><u>%SystemRoot%\History</u></b> <i>folder, subfolders, and files</i></p> <p>(U) History folder for web browsing.</p>	Administrators Authenticated Users CREATOR OWNER SYSTEM	Full Control Read, Write, Execute Full Control Full Control
<p><b><u>%SystemRoot%\Imapiud.ini</u></b> <i>file</i></p> <p>(U) File needed for Outlook Express.</p>	Administrators Authenticated Users CREATOR OWNER SYSTEM	Full Control Modify Full Control Full Control
<p><b><u>%SystemRoot%\Insreg.dat</u></b> <i>file</i></p> <p>(U) File needed for Netscape.</p>	Administrators Authenticated Users CREATOR OWNER SYSTEM	Full Control Modify Full Control Full Control

<b>FOLDER OR FILE</b>	<b>USER GROUPS</b>	<b>RECOMMENDED PERMISSIONS</b>
<p><b><u>%SystemRoot%\Profiles</u></b>  <i>folder, subfolders, and files</i></p> <p>(U) Contains user profile settings. Because the Profiles folder needs to retain specific user permissions, it will be configured manually in Chapter 7.</p>	Ignore	
<p><b><u>%SystemRoot%\regedit.exe</u></b>  <i>file</i></p> <p>(U) Registry editing tool.</p>	Administrators SYSTEM	Full Control Full Control
<p><b><u>%SystemRoot%\repair</u></b>  <i>folder, subfolders, and files</i></p> <p>(U) Backup files of SAM database and other important registry and system files to be used during a system repair.</p>	Administrators SYSTEM	Full Control Full Control
<p><b><u>%SystemRoot%\Security</u></b>  <i>folder, subfolders, and files</i></p> <p>(U) SCM databases and templates.</p>	Administrators SYSTEM	Full Control Full Control
<p><b><u>%SystemRoot%\SendTo</u></b>  <i>folder, subfolders, and files</i></p> <p>(U) Folder needed for Outlook Express.</p>	Administrators Authenticated Users CREATOR OWNER SYSTEM	Full Control Read, Write, Execute Full Control Full Control
<p><b><u>%SystemRoot%\Temporary Internet Files</u></b>  <i>folder, subfolders, and files</i></p> <p>(U) Folder needed for web browsing</p>	Administrators Authenticated Users CREATOR OWNER SYSTEM	Full Control Read, Write, Execute Full Control Full Control

**(U) Table 11 Recommended File System Settings**

(U) **NOTE:** After making any modifications to the configuration files make sure the changes are saved (See Chapter 4) and then test the changes before installing them on an operational network.

## (U) Running Security Configuration Files

(U) Once the appropriate configuration file(s) have been modified, security analysis and configuration can be performed via the GUI or the command line program. Batch files to perform command line options are included with the companion CD and are the recommended method for configuration.

**(U) WARNING:** Applying a secure configuration to a Windows NT system may result in a loss of performance and functionality.

### (U) SCM Databases

(U) The SCM uses a database to store configurations for an analysis or configuration. To open an existing database or new database while using the GUI:

- In the MMC, right click on the **Database** node
- Select **Open Database**
- Enter the name of an existing database or a new database
- Click **Open**

**(U) NOTE:** It is recommended that a new database be created for each analysis and configuration coupling.

(U) Configuration files may be imported into the database by executing the following procedure:

- If a new database name was entered when opening a database, you will automatically be prompted to enter the configuration file to import. Otherwise:
  - Right click on the **Database** node
  - Select **Import Configuration**
- In the **Select Configuration to Import** dialog box, select the appropriate *inf* configuration file.
- Check the **Overwrite existing configuration in database** box to remove any previous settings stored in the database.

**(U) NOTE:** Import operations can append to or overwrite database information that has been previously imported. Appending is the default. Check the "Overwrite existing configuration in database to overwrite the current database.

**(U) WARNING:** To avoid confusion and accidental combining of configurations, it is recommended that this option be checked every time a new analysis or configuration is performed.

- Click **Open**

**(U) SCM Command Line Options**

(U) The command line syntax for the SCM is:

```
secedit {/analyze | /configure} [/cfg filename] [/db filename]
[/log LogPath] [/verbose] [/quiet] [/overwrite] [/areas Areas]
```

(U) The parameter explanation follows:

- The first parameter specifies the type of operation to perform. Besides the two listed here, two other options exist, but are not detailed in this guide. The following are used in this chapter:
  - /analyze - performs an analysis
  - /configure – performs a configuration
- /cfg filename - Path to a configuration file that will be appended to the database prior to performing the analysis.
- /db filename - Path to the database that SCE will perform the analysis against. If this parameter is not specified, the last configuration/analysis database is used. If there is no previous database, %SystemRoot%\Security\Database\secedit.sdb is used.
 

**(U) NOTE: It is recommended that a new database be created for each analysis and configuration coupling.**
- /log LogPath - Path to log file for the process. If not provided, progress information is output to the console.
 

**(U) NOTE: Log information is appended to the specified log file. You must specify a new file name if you want a new log file to be created.**
- /verbose - Specify detailed progress information.
- /quiet - Suppress screen and log output.
- /overwrite – Overwrite the named database with the given configuration information.
 

**(U) NOTE: Configuration files can be appended to or overwrite database information that has been previously created. Appending is the default. Specify the /overwrite option to overwrite the current database.**

**(U) WARNING: To avoid confusion and accidental combining of configurations, it is recommended that this option be included every time a new analysis or configuration is performed.**
- /areas Areas – Only relevant when using the /configure switch. Specifies the security areas to be processed. The following areas are available:
  - SECURITYPOLICY - Local policy and domain policy for the system, including account policies, audit policies, etc.
  - GROUP\_MGMT - Restricted Group settings
  - USER\_RIGHTS - User rights assignments
  - DSOBJECTS - Security on directory objects
  - REGKEYS - Security permissions on local registry keys
  - FILESTORE - Security permissions on local file system
  - SERVICES - Security configuration for all defined services.

(U) NOTE: If the `/areas` switch is not used, the default is all security areas. If used, each area name should be separated by a space.

## (U) Performing a Security Analysis

(U) A security analysis is performed against a database. The configuration file(s) that have been imported into the database define the *baseline* for the analysis. Security settings within the configuration file(s) are compared to the current system security settings and the results are stored back into a database. The baseline settings are presented alongside the current system settings. Configuration information can be modified as a result of the analysis. The modified configuration information can be exported into a configuration file for subsequent use.

### (U) Performing a Security Analysis via the Command Line

(U) To perform a security analysis via the command line, execute the following in a CMD prompt window:

```
□ secedit /analyze [/cfg filename] [/db filename] [/log LogPath]
  [/verbose] [/quiet] [/overwrite] [>> results_file]
```

(U) *results\_file* is the name of a file to contain the analysis results. This is especially useful for reviewing the results at a later time. If the `>> results_file` is omitted, output will be written to the screen.

### (U) Performing a Security Analysis via the GUI

(U) The following steps should be followed to perform a security analysis via the GUI:

- If a new database was opened and a configuration file was imported, the Perform Analysis dialog box will automatically appear. Otherwise:
  - Right-click on the **Database** node
  - Select **Analyze System Now...**
- In the **Perform Analysis** dialog box, enter the error log file path.
 

(U) NOTE: Log information is appended to the specified log file. You must specify a new file name if you want a new log file to be created.
- Click **OK**

## (U) Configuring a System

(U) During configuration, errors may result if specific files or registry keys do not exist on the system, but exist in the *inf* configuration file. Do not be alarmed. The *inf* files attempt to cover many different scenarios and configurations that your system may or may not match.

### (U) Configuring a System via the Command Line

(U) To configure all of the available security options at one time via the command line:

```
□ secedit /configure [/cfg filename] [/db filename] [/log
  LogPath] [/verbose] [/quiet] [/overwrite] [/areas Areas]
```

# UNCLASSIFIED

**(U) WARNING:** Failure to enter a new database name each time a configuration is made may result in unpredictable behavior by the SCM. Since the SCM by default uses a default database (secedit.sdb) as a baseline for analysis, the imported configuration file could get merged with this baseline and report unreliable analyses.

- Reboot the computer

(U) Following is an example of using the command line tool to configure only specific security areas:

- `secedit /configure /cfg workstation.inf /db newdb.sdb /log logfile.txt /overwrite /areas REGKEYS FILESTORE`

(U) This example will import the `workstation.inf` configuration file into the `newdb.sdb` database and apply the file system and registry permission security settings specified in the `workstation.inf` configuration file to the local system.

(U) Several batch files to automatically configure systems using the configuration files provided are included on the companion CD. All can be run from a command line. These files are:

<b>File Name</b>	<b>Configuration File Used</b>
PDC.BAT	PDC.inf
BDC.BAT	BDC.inf
WS.BAT	Workstation.inf
MEMBER.BAT	MemberServer.inf
EXCHANGE.BAT	Exchange.inf

## **(U) Configuring a System via the GUI**

(U) The following steps should be followed to configure a system using the SCM:

- Right-click on the **Database** node
- Select **Configure Now....**
- In the **Configure System** dialog box, enter the error log file path.

**(U) NOTE:** Log information is appended to the specified log file. You must specify a new file name if you want a new log file to be created.

- Click **OK**
- Reboot the computer.

## (U) Manual Settings

(U) There are many settings that must also be done manually to secure a Windows NT system. These settings are listed and described in the following sections.

### (U) Manual Registry Changes

(U) In addition to the registry permissions set with the SCM in Chapter 5, there are several other recommended registry modifications to ensure greater system security.

**(U) WARNING: Incorrect registry modifications can severely impair or disable a Windows NT system. Currently, there is no Undo command for deletions within the registry. The registry editors prompt for confirmation of deletions if Confirm On Delete is selected from the Options menu. When deleting a key, the message does not include the name of the key being deleted. Therefore, check the selection carefully before proceeding.**

#### (U) Running the Registry Editor

(U) Windows NT comes with two registry editors, Regedit.exe and Regedt32.exe.

(U) Regedit.exe is based on the Windows 95 registry editor and does not have facilities for modifying permissions. Therefore, the Windows NT registry editor, Regedt32.exe, should always be used to make changes in the Windows NT registry.

(U) To start the Windows NT registry editor:

- Log on as an administrator
- Select **Start** → **Run...**
- Type Regedt32.exe in the **Open** dialog box
- In the registry editor, go to the **Options** menu
- Verify that **Confirm on Delete** is checked

#### (U) Disabling CDROM Autorun

(U) By default Windows NT autoruns any CDROM that is placed in the drive. This allows executable content to be run without any access to the command prompt. The following instructions disables this:

Hive: HKEY\_LOCAL\_MACHINE  
Key: \System\CurrentControlSet\Services\Cdrom  
Name: Autorun  
Type: REG\_DWORD  
Value: 00000001

## UNCLASSIFIED

- Select the **HKEY\_LOCAL\_MACHINE on Local Machine** window
- Navigate down the **\System\CurrentControlSet\Services\Cdrom** path, double clicking on each key along the way
- Select the **Cdrom** key
- Select **Add Value...** from the **Edit** menu
- Enter `AutoRun` for **Value Name**:
- Select **REG\_DWORD** from the Data Type: drop down list
- Click **OK** in the Add Value window
- Enter `00000001` for the Data: value in the DWORD Editor
- Click **OK** to close the DWORD Editor

### **(U) Removing Registry Keys**

(U) For each key value to be removed, perform the following steps:

- Select the key to be removed
- From the **Edit** menu select **Delete**
- Click **Yes** in the **Warning** window

### **(U) Removing Subsystem Registry Keys**

(U) To fully prevent any OS/2 or POSIX based attacks, all registry keys dealing with these subsystems must be removed. Even if the subsystem executables have been removed from the `%SystemRoot%\system32` folder, the subsystem could be reactivated if the registry keys still exist.

(U) Remove the following key values related to the OS/2 subsystem:

- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment\Os2LibPath`
- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems\Os2`

(U) Remove the following key value related to the POSIX subsystem:

- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems\Posix`

## **(U) Manual Folder and File Permission Changes**

(U) Several folder permissions must be manually set. Additionally, several files related to the OS/2 and POSIX subsystems must be removed.

### **(U) Setting Folder and File Permissions**

(U) To set permissions on an individual folder or file:

- In explorer, right click on the folder or file
- Select **Properties** in the pull-down menu
- In the **Properties** dialog box, select the **Security** tab

# UNCLASSIFIED

- All of the folder permission settings below are being manually set because they should not inherit permission attributes from their parent folders. Therefore, uncheck the **Allow inheritable permissions from parent to propagate to this object** checkbox.
- Click on the **Remove** button in the **Security** dialog box.
- Add/remove users and groups to reflect the recommended permissions.
- For each user and/or group, set the permissions by clicking on the permission checkboxes.
- If the folder permissions should encompass the folder itself, all files within the folder, and all subfolders
  - Click the **Apply** button
  - Click **OK**. Stop here.
- Otherwise, click the **Advanced** button.
- Double-click on a user and/or group. A **Permission Entry** dialog box will appear.
- In the **Apply** onto pull-down menu, select the correct configuration (e.g. **This folder only**).
- Click **OK** to exit the **Permission Entry** dialog box.
- Click **Apply** in the **Advanced** dialog box.
- Click **OK** in the **Advanced** dialog box.
- Click **OK** in the **Properties** dialog box.

## (U) Recommended File and Folder Permissions

<b>FOLDER OR FILE</b>	<b>USER GROUPS</b>	<b>RECOMMENDED PERMISSIONS</b>
<b>%SystemRoot%\\$NtUninstall*</b> (all uninstall folders) <i>folder, subfolders, and files</i>  (U) Contains uninstall files for hotfixes and other applications.	Administrators SYSTEM	Full Control Full Control
<b>%SystemRoot%\Profiles</b> <i>folder only</i>  (U) Contains user profiles and desktop settings.	Administrators Authenticated Users CREATOR OWNER SYSTEM	Full Control Read, Execute Full Control Full Control
<b>%SystemRoot%\Profiles\Administrator or profile of renamed Administrator account</b> <i>folder, subfolders, and files</i>  (U) Administrator profile.	Administrators SYSTEM	Full Control Full Control
<b>%SystemRoot%\Profiles\All Users</b> <i>folder, subfolders, and files</i>  (U) Common profile settings for all users on the system.	Administrators Authenticated Users SYSTEM	Full Control Read, Execute Full Control
<b>%SystemRoot%\Profiles\Default User</b> <i>folder, subfolders, and files</i>  (U) Default profile for users logging on for the first time.	Administrators Authenticated Users SYSTEM	Full Control Read, Execute Full Control

**(U) Table 12 Recommended File Folder Permissions**

**(U) Removing Existing Folders and Files**

(U) The OS2 and Posix subsystems in Windows NT can introduce security vulnerabilities to the operating system. Therefore, remove the following files and folder from the %SystemDirectory% (%SystemRoot%\system32) folder:

- os2.exe
- os2ss.exe
- os2srv.exe
- psxss.exe
- posix.exe
- psxdll.dll
- The \os2 folder.

(U) If the system has been upgraded to Windows NT 4.0 from a DOS system:

- Remove the %SystemDrive%\DOS folder and all files within this folder.

**(U) Share Permissions**

(U) Windows NT shares are a means by which files, folders, printers, and other resources can be published for network users to remotely access. Regular users cannot create shares on their local machines; only Administrators and Power Users have this ability and must have at least List permission on the folder to do so. Since shares may contain important data and are a window into the local system, care must be taken to ensure proper security settings on shared resources.

(U) The following share permissions can be granted to users or groups:

- No Access
- Read
- Modify
- Full Control

(U) Share permissions are granted independent of NTFS permissions. However, share permissions act aggregately with NTFS permissions. When accessing a remote share, the more restrictive permissions of the two apply. For example, if a user accesses a share remotely and has Full Control over a shared folder, but only NTFS Read access to that folder on the local file system, he will only have Read access to the share.

(U) The default permissions on a share give the Everyone group Full Control; therefore, you must explicitly edit security permissions on shared resources to limit share access.

**(U) Setting Share Permissions**

(U) To create a share and set security permissions:

- In explorer, right mouse-click on the folder that is to be shared.
- Select the **Sharing...** menu option
- Click the **Shared As** radio button.

- Specify the **Share Name**.
- Click the **Permissions** button.
- Add, remove, or edit the users and/or groups in the access control list for the share.

**(U) Share Security Recommendations**

(U) When creating shares and share permissions, adhere to the following criteria when possible:

- Ensure that the Everyone group is not given Full Control permissions on any shares.
- Use the Authenticated Users group in place of the Everyone group.
- Give users and/or groups the minimum amount of permissions needed on a share.
- To protect highly sensitive shares not for general use, hide shares by placing a \$ after the share name when creating a share. Users can still connect to hidden shares, but must explicitly enter the full path to the share (i.e. the share will not be visible in Network Neighborhood).

(U) (U) Table 13 lists the recommended printer share security settings.

<b>Share</b>	<b>Settings</b>
<b>(U) Printer Share</b>	Authenticated Users: Print Administrators: Full Control SYSTEM: Full Control CREATOR OWNER: Full Control

**(U) Table 13 Recommended Printer Share Settings**

**(U) Auditing**

(U) Auditing is critical to maintaining the security of a domain. Windows NT includes auditing capabilities that collect information about the system usage including application, system, and security events.

**WARNING: Auditing can consume a large amount of processor time and disk space. It is recommended that administrators check, save and clear audit logs as necessary to reduce the chances of system degradation.**

**(U) File System Auditing**

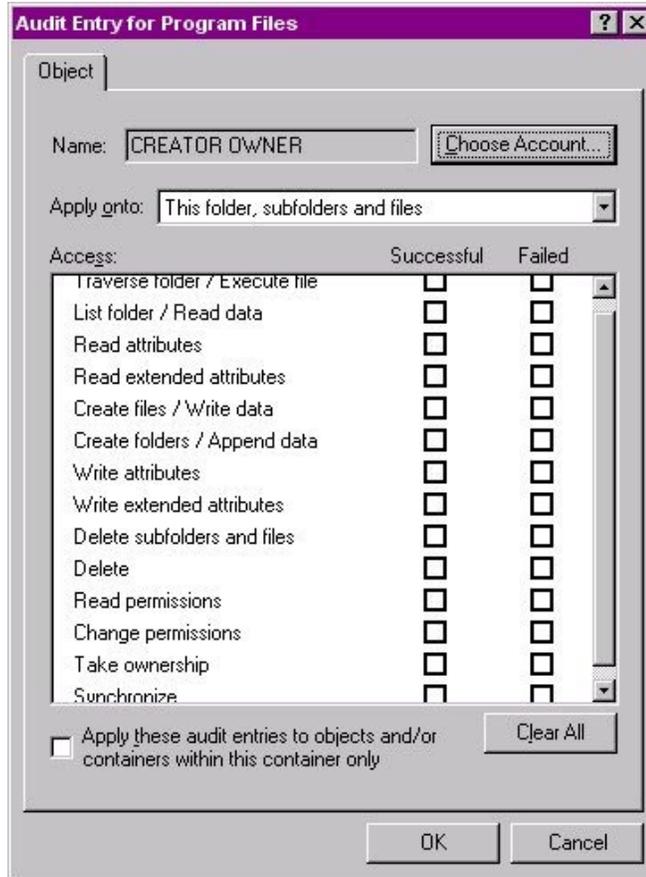
(U) File System Auditing tracks a particular user's use of a specific directory or file.

**NOTE: this can only be set via Windows NT Explorer**

(U) To enable file system auditing:

- Select **Start** → **Programs** → **Windows NT Explorer**
- Select a drive or folder to be audited
- Right click on the object to open its **Context menu**
- Select **Properties**
- Select **Security** tab
- Click **Advanced** button
- Select **Audit** tab

- Click the **Add...** button
- Choose a user or group by selecting the name
- Click the **Add** button
- Click the **OK** button (See (U) Figure 11 for a list of auditable events)



**(U) Figure 11 Auditable Events**

- Select events to audit.
- To Audit the Directory Only:
  - In the **Apply onto** option: Change the pull down bar to **This folder only**
- To Audit Directories and Its Files Only:
  - In the **Apply onto** option: Change the pull down bar to **This folder and files**
- To Audit the Directory and Subdirectories Only, Not Files:
  - In the **Apply onto** option: Change the pull down bar to **This folder and subfolders**
- To Audit Directories, Subdirectories, And All Files:
  - In the **Apply onto** option: Change the pull down bar to **This folder, subfolders and files**

**(U) NOTE: Only new files and directories inherit auditing lists from the directory in which they are created. To ensure that access to existing files will be audited, be sure to select both Replace Auditing on Subdirectories and Replace Auditing on**

# UNCLASSIFIED

Existing Files in the Directory Auditing dialog box when creating a directory auditing list.

- ❑ Click **OK** to close the **File Auditing** window
- ❑ Click **OK** to close the **Listings** window
- ❑ Click **OK** to close the **Properties** window

## (U) Auditing Registry Changes

Auditing of registry keys can track changes made by users or applications.

To enable registry auditing:

- ❑ Select **Start** → **Run...**
- ❑ Type Regedt32.exe in the **Open** dialog box
- ❑ Click on a key to audit
- ❑ Select **Auditing** from the **Security** menu (See (U) Figure 12 for the dialog box)



(U) Figure 12 Registry Key Auditing Dialog Box

- ❑ Click the **Add...** button
- ❑ Select the appropriate domain in the **List Names From:** drop down list
- ❑ Select a user account or group account to audit
- ❑ Click **Add**
- ❑ Click **OK** to close the **Add Users and Groups** window
- ❑ Select events to audit described below in the **Events to Audit** portion of the dialog box ((U) Table 14 lists and describes the audit events)

<b>Audit Option</b>	<b>Audit Event Description</b>
Query Value	Open a key with Query Value access
Set Value	Open a key with Set Value access
Create Subkey	Open a key with Create Value access
Enumerate Subkeys	Open a key with Enumerate Subkeys access (that is events that try to find the subkeys of a key)
Notify	Open a key with notify access
Create Link	Open a key with Create Link access
Delete	Delete the key
Write DAC	Determine who has access to the key
Read Control	Find the owner of a key

**(U) Table 14 Registry Audit Events**

**(U) Managing the Event Logs**

(U) Event logs indicate particular events that have transpired. The Security, Application, and System event logs contain information generated by the specified audit settings.

(U) Auditing too many events can cause the event logs to reach capacity quickly. If the event logs become full, the system administrator must save and clear the event logs more frequently than required. Having too much data in the event logs also makes it more difficult to examine the logs for possible security breaches.

**(U) NOTE:** The event logs should be saved and cleared on a daily basis for the above-mentioned reasons.

**(U) Saving and Clearing the Event Logs**

- Select the appropriate event log from the **Log Menu**
- Select **Clear All Events** from the **Log** menu
- Click **Yes** to save settings
- Enter a unique file name
- Click the **Save** button
- Click **Yes** to clear the event log
- Repeat the above steps for each log

**(U) Resetting the Event Log Settings after the System Halts**

(U) If the system halts as a result of a full log, an administrator must restart the system and clear the log.

**(U) Note:** Before clearing the security log, save the data to disk.

(U) Use the Registry Editor to modify the following Registry key value:

Hive: **HKEY\_LOCAL\_MACHINE**  
 Key: **\System\CurrentControlSet\Control\Lsa**  
 Name: **CrashOnAuditFail**  
 Type: **REG\_DWORD**  
 Value: **1**

- Log on as an administrator

## UNCLASSIFIED

- Select **Start** → **Run...**
- Type Regedt32.exe in the **Open** dialog box
- Navigate down the `\System\CurrentControlSet\Control\Lsa` path, double clicking on each key along the way
- Double click the **CrashOnAuditFail** key
- Enter **1** in the DWORD editor
  - (U) **NOTE:** This value is set by the operating system just before it crashes due to a full audit log. While the value is 2, only the administrator can log on to the computer. This value confirms the cause of the crash. Reset the value to 1
- Click **OK** to continue
- Exit the registry editor

UNCLASSIFIED

This Page Intentionally Left Blank

UNCLASSIFIED

## (U) Disaster Recovery

(U) Malicious users not only threaten the integrity but the very existence of data. Hard disk crashes, power failures, erroneous key strokes, and viruses can also destroy valuable data and systems. The need for system backups and a disaster recovery plan can not be overstated. A disaster recovery plan should be tested on a regular basis. The first attempt to restore a system should not be after a major failure.

### (U) Emergency Repair Disk

(U) The Emergency Repair Disk (ERD) is a critical part of the recovery process that helps system administrators recover the Windows NT configuration from a normally unrecoverable state. The ERD contains the hives of the registry, copies of the MS-DOS subsystem initialization files (`autoexec.nt` and `config.nt`), and the SAM database. When making a major change to the system, two copies of the ERD should be made, one before and one after the change. Examples of major changes include; adding, removing, or modifying hard drives, partitions, file systems, registry configurations, or software. Periodic updates of the ERD should be part of the standard operating procedures.

(U) The ERD assists in recovery by:

- Repairing bad registry data
- Restoring corrupted or missing files on the system partition
- Replacing a corrupt Kernel, which is the core of the Windows NT operating system
- Replacing a bad boot sector for a FAT partition

(U) The ERD is not a complete solution for recovering the system. A Backup utility must be used in conjunction with the ERD to fully recover from a disaster. The ERD:

- Does not contain a full backup of the registry
- Cannot fully restore the system partition information
- Cannot repair unmountable partitions except for the system partition (normally C:)
- Does not replace a damaged NTFS boot sector.

### (U) Modifying Window NT 4.0 Setup Disk for Use with a Post Service Pack 4 ERD

(U) The original Windows NT Setup Disks do not properly allow the use of an ERD made after applying Service Pack 4 on a system. To correct this:

- Obtain the three Windows NT version 4.0 Setup Disks

(U) **NOTE:** These disks can be created using the Windows NT version 4.0 installation CD ROM by opening a command prompt and typing `winnt32 /ox` (on a Windows NT system) or `winnt /ox` (on a DOS based system) within the `\i386` directory.

## UNCLASSIFIED

- Copy `Setupdd.sys` from Service Pack 4 to the Windows NT version 4.0 Setup Disk 2

(U) **WARNING:** This file must be copied for successful recovery using an ERD. For more information see Microsoft Knowledge Base article Q168015.

### (U) Creating an Emergency Repair Disk

(U) A blank diskette is required when creating an ERD (`Rdisk.exe`, always formats the floppy disk). To create the ERD:

- Insert a 3.5 inch, 1.44 MB floppy disk into the A: drive
- Select **Start** → **Run...**
- Type `rdisk /s` in the Open dialog box

(U) **NOTE:** The `/s` option saves all of the current configuration settings including user accounts and file permissions. The saved repair info is saved in the `\%SystemRoot%\repair` directory.

- Click **OK** to continue
- Click **Yes**
- Click **OK** in the following **Setup** window
- After the ERD has successfully been created, the following screen will appear
- Click **OK**
- Store the disk in a safe and secure place

### (U) Recovering the System Using an Emergency Repair Disk

(U) The recovery process uses both the ERD and the original files from the Windows NT installation CD ROM. Consequently, Service Pack 4 and all the previously installed hot fixes must be reinstalled after recovering with the ERD. For further information on using the ERD, see the Microsoft Knowledge Base at <http://www.microsoft.com> and search for article Q146887.

**NOTE:** To use the Emergency Repair Disk utility, you must have the updated version of `Setupdd.sys`. The updated version is contained in SP4. To update your version of `Setupdd.sys`, copy `Setupdd.sys` from the Service Pack to your Windows NT 4.0 Setup Disk 2 from the original product media. This will replace the older version of `Setupdd.sys` with the updated version. For more information, consult the Knowledge Base at <http://support.microsoft.com/support/> and search for KB article Q158423.

- Insert the **Windows NT Setup Disk 1** into the A: floppy drive
- Reboot system
- Press **R** To repair a damaged Windows NT version 4.0 installation
- Ensure all tasks are marked with an **X**
- Press **Enter** to continue (perform selected tasks)
- Specify all mass storage devices in the system
- Press **Enter** to continue

## UNCLASSIFIED

- Press **Enter** to confirm that the ERD is available
- Place the ERD in the A: floppy drive when prompted
- Press **Enter** to continue
- Select all registry files with an **X**
- Press **Enter** to continue (perform selected tasks)
- Press **A** to replace the non-original files
- Follow the remaining on screen instructions
- After repair is complete, reapply Service Pack 4 and all previously installed hotfixes as described in Chapter 3

### **(U) Application Problems**

(U) The settings described in the guide are designed for programs installed on a separate partition from the %systemroot%\ directory. However, if applications stop working as a result of locking down the system according to the guide, use the following troubleshooting checklists.

#### **(U) General Application Troubleshooting**

- (U) Make sure the administrator is installing the application and the administrator can run the application successfully
- (U) Check permissions on the directories the applications are installed in. The permissions should allow Authenticated Users read and execute permissions.
- (U) Check permissions on the following directories and any files that the installation program added to these directories:
  - \\%SystemRoot%\system32\
  - \\%SystemRoot%\system\
  - \\%SystemRoot%\
- (U) Ensure that the appropriate files in these directories allow Authenticated Users read and execute permissions
- (U) Check the permissions on the icons that were made by the setup program. They should also have the read and execute permissions.
- (U) If the program is still not working, check the permissions in the registry keys for the application found in **HKEY\_LOCAL\_MACHINE\SOFTWARE**

### **(U) Domain Backup Policy**

(U) To protect both the operating system and data, it is critical to perform regular backups of the operating system, application files, and user data. Back up privileges should be limited to Administrators and Backup operators—people who can be trusted with read and write access on all files. There are five types of backup that can be performed on either the server or the workstation: normal, incremental, differential, copy and daily.

- (U) **Normal backup:** Archives all selected files and marks each as having been backed up. This method of backup allows for the fastest restoration because it has the most recent files on it.
- (U) **Incremental backup:** Archives only those files created or changed since the last normal backup. It also unsets the archive attribute. This method saves time during the subsequent incremental backups, but makes the restoration more complex. When restoring, a combination of normal and incremental backups must be used. The normal backup must first be restored, then all incremental backups in the proper order.
- (U) **Differential backup:** Archives only those files that have been created or changed since the last normal backup. This method does not mark the files as backed up; it relies on the integrity of the last normal backup records. If using differential backups, the normal backup must first be restored, then only the most recent differential backup.
- (U) **Copy backup:** Archives all selected files, but does not mark the files as having been backed up. A copy backup is particularly useful when backing up files between a scheduled incremental backup and the last normal backup. By not marking the files, it allows the normal markings of an incremental backup to remain valid.
- (U) **Daily backup:** Archives all of the selected files that have been modified on that day, but it does not mark the files as being backed up.

## (U) Security Implications

(U) Although Administrators have full privileges, they do not, by default, have access to all files. Rather, they have the ability to take ownership of all files; once this takes place, they may grant themselves rights to the files.

(U) The right to perform backups, identified by users in the Backup Operators group, is one of the most powerful rights that administrators can assign. Backup operators are able to read and write to any file in the system, regardless of the rights assigned to it. Backup and restore rights permit users to circumvent the file access restrictions present on Windows NT NTFS disk drives for the purpose of backup and restore. **This right should be granted only when there is a clear need for it; even then, it should be limited to only a few trusted users.** Although users with backup rights cannot read the files they back-up directly, they can restore these files on another system.

(U) Several things to consider when preparing a backup policy:

- Secure the `backup.log` file by placing permission restrictions on it
- When restoring from a backup, ensure that the NTFS permissions remain intact
- If possible, copy the `backup.log` file to another system or to removable media
- Members of the Backup Operators group should have special logon accounts, not regular user accounts
- Set restrictions on the backup account, such as forcing the user to log on from a particular system only during appropriate hours
- Determine the data and systems to be backed up
- Determine the frequency of scheduled backups

## (U) Network Security

(U) After installing Windows NT Server or Workstation, it is imperative to minimize the security risk to your network domain. The security implications of Domain Name System (DNS), Windows Internet Name Service (WINS), Dynamic Host Configuration Protocol (DHCP), Terminal Emulation Protocol (Telnet), and File Transfer Protocol (FTP) servers will be discussed.

### (U) Default Network Protocols

(U) Microsoft provides native support for three protocols to perform local or wide area networking. These protocols are NetBIOS Extended User Interface (NetBEUI), NWLink/IPX, and TCP/IP.

(U) **NetBEUI** is Microsoft's own network protocol and is designed for small networks. NetBEUI is non-routable, broadcast-based, and is sometimes used as a legacy protocol for networking between LAN Manager, LAN Server, and Windows for Workgroups.

(U) **NWLink/IPX** is Microsoft's implementation of Novell's IPX/SPX protocol. It is designed to provide interconnectivity between Novell NetWare Servers and Clients and Windows NT/Windows 95. NWLink/IPX is fully routable and provides for efficient data transfers over both local and wide area networks. This protocol should be used only if there are Novell Servers or Clients within the domain.

(U) **TCP/IP** is the standard and primary protocol of the Internet. It is fully routable and supports communications between multiple operating systems such as Unix, Windows NT, and Windows 95. TCP/IP is a directed protocol that eliminates most of the broadcast traffic associated with the NetBEUI and NWLink/IPX protocols. Windows NT supports more traditional TCP/IP services, such as FTP and Telnet.

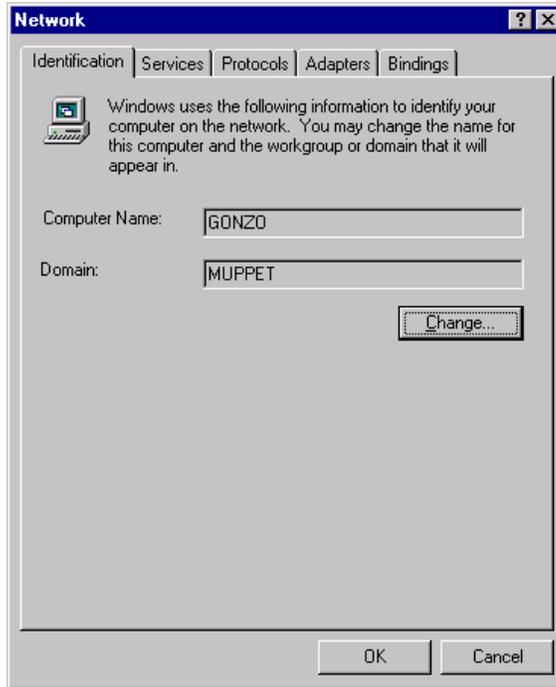
(U) Implementation of only the TCP/IP protocol is recommended in order to support compatibility when connecting to other heterogeneous domains while minimizing the number of active network protocols.

### (U) Configuring Network Components

#### (U) Adding Workstations/Servers to the Domain

- Select **Start** → **Settings** → **Control Panel**
- Double click the **Network** icon
- Ensure the **Identification** tab is selected
- Click the **Change...** button
- Verify that the computer name is listed in the **Computer Name:** field
- Ensure the **Domain** radio button is selected

- Enter the domain name in the **Domain:** field
  - Check the **Create a Computer Account in the Domain** checkbox
  - Enter an Account Operator's username in the **User Name:** field
  - Enter an Account Operator's password in the **Password:** field
- (U) WARNING: Domain Administrator account(s) should never be used to add workstations or servers to the domain from the new computer.**
- Click **OK** to continue

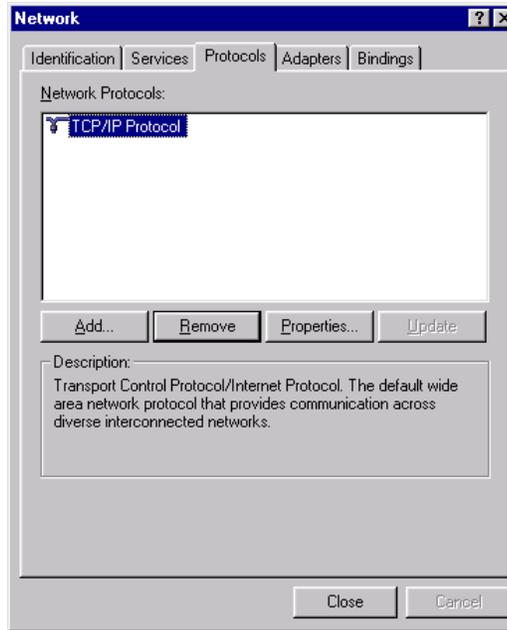


**(U) Figure 13 Identification Tab of Network Window**

### **(U) Configuring Network Protocols**

- Select the **Protocols** tab
- Remove the NetBEUI and NWLink/IPX protocols with the **Remove** button
- If the TCP/IP protocol is not listed, then click the **Add** button and choose the TCP/IP protocol

**(U) NOTE: TCP/IP should be the only active protocol on the network.**

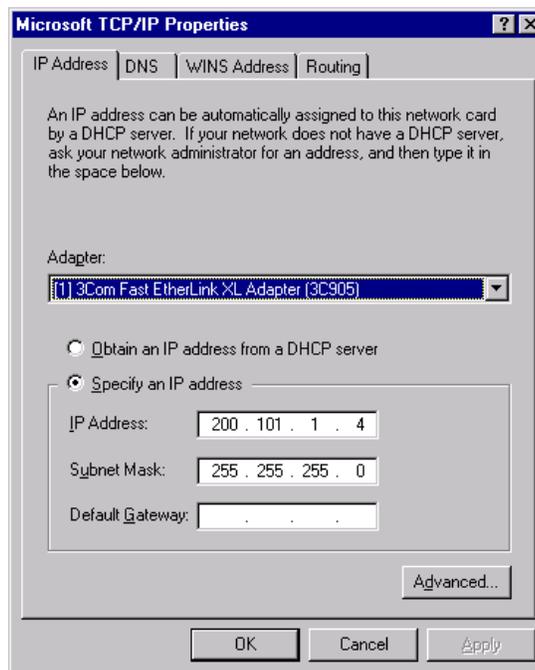


(U) Figure 14 Protocols Tab of Network Window

- Select the **Properties** button
- Ensure the correct adapter is selected
- Click the **Specify an IP address** radio button

**(U) WARNING: If not configured properly, the DHCP service introduces inherent security related accountability problems. Refer to Microsoft's configuration guidelines when using this service.**

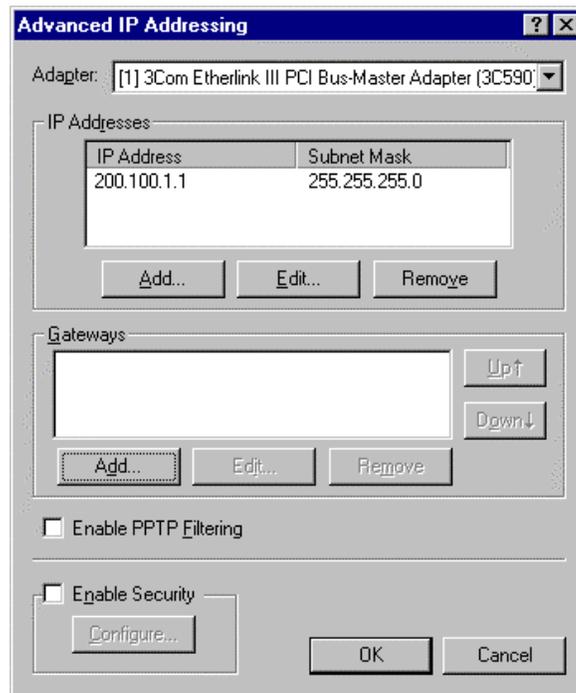
- Ensure that the **IP Address**, **Subnet Mask**, and **Default Gateway** fields are set correctly



(U) Figure 15 TCP/IP Properties Window

- Click the **Advanced...** button
- Ensure the **Enable PPTP Filtering** box is unchecked
- Ensure the **Enable Security** box is unchecked

**(U) WARNING:** All packet filtering should be done at the firewall to prevent unauthorized access from outside the domain.



**(U) Figure 16 Advanced IP Addressing Window**

- Click **OK** to exit **Advanced IP Addressing** window
- Click **OK** to close **TCP/IP Properties** window
- Click **OK** to close **Network** window
- Restart system

## **(U) Remote Access Service**

(U) Remote Access Service (RAS) provides a means for a remote Windows NT system to connect to a LAN via a dial-up connection. RAS allows Windows NT networks to be extended beyond the physical boundaries of an office or site. This is a remote node connection - the local system residing on the network is acting as a router for the remote Windows NT system. All traffic to/from the remote system passes through the local system with all application processing taking place at the remote system.

(U) RAS consists of a server and a client portion. The server authenticates the client and manages the connection. RAS provides mechanisms to protect a potentially insecure connection between server and client. To take full advantage of the RAS security mechanisms, a RAS server must be used in conjunction with a RAS client. These mechanisms include authentication, link encryption, and dial-back functions.

**(U) RAS Authentication**

(U) Authentication is the validation of a user's logon credentials. Since the connection between local and remote systems may take place over unsecured lines, Windows NT provides mechanisms to protect against "replay" type attacks.

(U) RAS provides three authentication protocols. Each protocol uses a different handshaking technique and may offer the use of various encryption algorithms. They are CHAP, SPAP, and PAP.

- **CHAP** (Challenge Handshake Authentication Protocol) is considered to be **the most secure of the three RAS authentication protocols**. One of two encryption algorithms can be chosen when using CHAP: DES or MD5. Although DES is the default option used by CHAP, MD5 is the recommended encryption algorithm.
- **SPAP** (Shiva Password Authentication Protocol) is a proprietary secure authentication scheme developed by Shiva Corporation.
- **PAP** (Password Authentication Protocol) should not be used. There is no encryption of the authentication process under PAP. It is primarily used when a client is not able to use one of the other more secure methods.

(U) A Windows NT RAS server can be configured to prevent local access to remote RAS systems not using CHAP or SPAP. This option is available in the **Remote Access Setup** dialog box.

(U) The authentication process can be made even more secure by requiring the addition of token-based authentication devices such as: challenge-response units, time-synchronization systems, smart cards, and biometric devices. These devices are available from third-party vendors.

**(U) RAS Link Encryption**

(U) Windows NT provides protection against data capture through link-based encryption. Link-based encryption will encrypt all network packets that are bound for a RAS link and decrypt all packets that have been received from RAS links. The algorithm used for providing link-based encryption in Windows NT is RSA Data Security's RC4.

**(U) RAS Dial-Back**

(U) Windows NT provides a built-in alternative to dial-back modems. RAS permits administrators to enable dial-back functions. The modem is not required to support dial-back functionality. Rather, the Windows NT RAS server authenticates the user, terminates the connection, and calls back the user at a prearranged number.

**(U) Secure Configuration of RAS**

(U) Before installing and configuring Windows NT RAS, considerations should be made as to which servers require the use of RAS. **RAS should only be installed on servers that require dial-up support.**

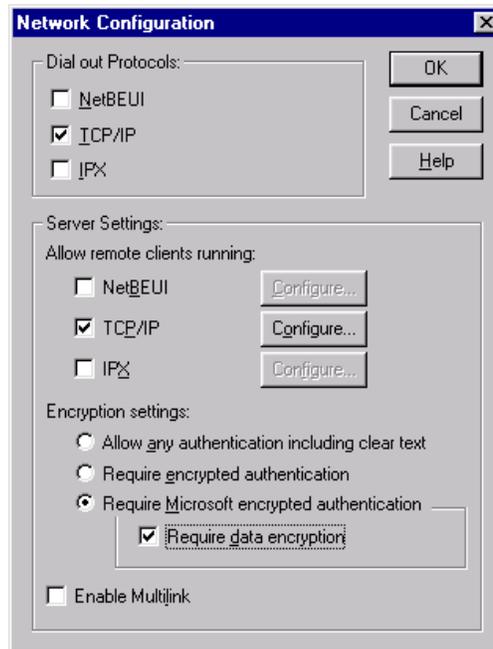
(U) Each Windows NT server can support 256 active RAS sessions, so centralization of modems is both feasible and cost-effective. More importantly, centralization provides the administrator with greater control over system security.

(U) Installing the RAS server on a Windows NT server will not automatically permit all users to use RAS. The right to use the RAS must be explicitly assigned by an administrator to individual users.

# UNCLASSIFIED

(U) **WARNING: Service Pack 4 and all recommended hotfixes, as described in Chapter 3, must be reapplied when RAS installation is complete.**

- Select **Start** → **Settings** → **Control Panel**
- Double click the **Network** icon
- Select the **Services** tab
- Highlight **Remote Access Service**
- Click **Properties...**
- Highlight the Port to configure
- Click the **Configure** button
- For a **RAS server**
  - Select **Dial out and Receive calls** in the **Port Usage** radio button
- For a **RAS client**
  - Select **Dial out only** in the **Port Usage** radio button
- Click **OK**
- Click **Network...**
- For a **RAS server** (See (U) Figure 17)
  - Ensure only the **TCP/IP** checkbox is checked in the **Dial out Protocols:** section
  - Ensure only the **TCP/IP** checkbox is checked in the **Server Settings:** section
  - Select the **Require Microsoft encrypted authentication** radio button
    - (U) **NOTE: This limits RAS clients to the use of CHAP authentication.**
  - Check the **Require data encryption** checkbox



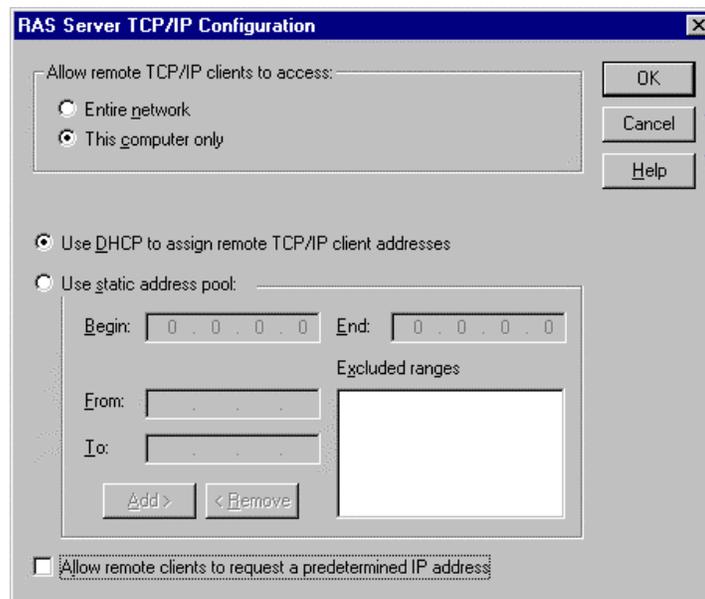
(U) Figure 17 Windows NT Server RAS Network Configuration

# UNCLASSIFIED

**(U) NOTE:** The use of link-based encryption is highly recommended, and will significantly increase the security of the RAS implementation. This forces all traffic between the RAS server and client to be encrypted using RSA Data Security's RC4 algorithm. This option is available only when using RAS with native NT clients and servers; it cannot be used with clients requiring either SPAP or PAP authentication.

- Click the **TCP/IP Configure...** button
- Verify the settings are correct in the **RAS Server TCP/IP Configuration** window (See (U) Figure 18)

**(U) NOTE:** It is strongly recommend that administrators allow remote access only to the local RAS server, and not to the entire network. This limits the potential of an intruder gaining access throughout an entire protected network. If users require access to additional resources, place the required resources on the RAS server.



**(U) Figure 18 RAS Server TCP/IP Configuration Window**

- Click **OK** to close the **RAS Server TCP/IP Configuration** window
- For a **RAS client**
  - Ensure only the **TCP/IP** checkbox is checked in the **Dial out Protocols:** section
- Click **OK** to close the **Network Configuration** window
- Click **Continue** to close the **Remote Access Setup** window
- Click **Close** to close the **Network** window

## **(U) RAS Permissions**

(U) By default, users are not permitted access to the RAS server remotely without explicit authorization from the system administrator. To allow remote user access to a RAS server:

- Select **Start** → **Programs** → **Administrative Tools (Common)** → **User Manager**
- Select the user account to be granted RAS dialin permission

- Click the **Dialin** button
- Check the **Grant dialin permission to user** checkbox
- Configure the Call Back settings appropriately

**(U) NOTE:** For the highest security and auditing tracking, the **Preset To:** setting is recommended. However, this setting may not allow the flexibility needed by roaming users. If this is the case, select the **Set By Caller** radio button to allow roaming users the ability to use remote access. This also allows the administrator the ability to audit the phone number being used to call into the domain.

**(U) WARNING:** It is recommended that user accounts that have dial-in access **NOT** have Administrator privileges. User accounts with Administrator privileges will have the ability to remotely modify the RAS Server – including the ability to change the restricted access to the local RAS Server and gain access to the entire network.

### **(U) Point-to-Point Tunneling Protocol**

(U) Windows NT includes the ability to create encrypted tunnels using the Point-to-Point Tunneling Protocol (PPTP). PPTP permits RAS to easily create and remove encrypted tunnels while connected to a RAS server. PPTP is an extension of Point-to-Point Protocol (PPP) which is currently supported by Windows 3.x, Windows 9x, Windows NT, Unix, and NetWare. PPTP creates a secure channel by tunneling, or encapsulating normal data in an encrypted envelope, thus creating a Virtual Private Network.

**(U) NOTE:** PPTP is usually not recommended unless all participants in the communication path have routers equipped to handle PPTP.

(U) To enable PPTP:

- Right-click on the **Network Neighborhood** icon
- Select **Properties**
- Select the **Protocols** tab
- Select the **TCP/IP** protocol
- Click the **Properties...** button
- Click the **Advanced...** button
- Check the **Enable PPTP Filtering** checkbox
- Click **OK** to close the **Advanced IP Addressing** window
- Click **OK** to close the **Microsoft TCP/IP Properties** window
- Click **OK** to close the **Network** window

### **(U) RAS Auditing**

(U) RAS can be enabled to generate records in the audit logs that indicate a number of activities, including normal connections, successful disconnection, successful callbacks, disconnects due to idle lines, timed-out authentication, and line errors. Excessive failed connections may indicate that someone is trying to break into an account. **Administrators should make use of the logging and auditing facilities available.** Setting a parameter in the Registry enables RAS auditing.

(U) The registry key value to enable this feature is:

# UNCLASSIFIED

Hive: HKEY\_LOCAL\_MACHINE  
Key: \System\CurrentControlSet\Services\RemoteAccess\Parameters  
Name: Enable Audit  
Type: REG\_DWORD  
Value: 1

- Select **Start** → **Run...**
- Type `Regedt32.exe` in the **Open** dialog box
- Select the **HKEY\_LOCAL\_MACHINE on Local Machine** window
- Navigate down the `\System\CurrentControlSet\Services\RemoteAccess\Parameters` path, double clicking along the way
- Double-click the **Enable Audit** key in the right pane
- Ensure the value in **Data:** field is **1**
- Click **OK** to close the **DWORD Editor**
- Exit the Registry Editor

## **(U) Other Network Security Concerns**

### **(U) FTP Server Service**

(U) The FTP Server Service allows users to access specific directories and files remotely. It is recommended that the FTP Server Service not be started on domain servers or workstations. Regular domain users should not be granted FTP access since there is already access via the shared domain directories through the Network Neighborhood icon. Files can still be transferred to and from non-Windows NT systems using the Windows NT FTP client.

(U) If required, configure a stand-alone FTP Server with the following recommendations:

- Create FTP accounts for each user
- Designate one physical disk as the FTP home directory

**(U) WARNING: FTP does not encrypt passwords. If users are allowed to FTP into the domain, user account names and passwords will be transmitted in the clear. Keep in mind that anonymous users are difficult to audit.**

### **(U) DNS Server Service**

(U) DNS Server Service enables name resolution for systems outside the domain. DNS Server Service is not normally configured during a typical installation. Starting the DNS Server Service is not recommended. Enabling this service with its default configuration can potentially render the server vulnerable. Service Pack 4 must be reapplied after starting this service. See Chapter 3 for proper installation procedures of Service Pack 4 and related hotfixes.

**(U) Telnet Server Service**

(U) By default, a Telnet Server Service is not included with Windows NT Workstation or Server. Third-party products are available to implement a Telnet Server Service. Starting any Telnet Server Service is not recommended.

**(U) WARNING: Telnet does not encrypt passwords. If users are allowed to Telnet into the domain, user account names and passwords will be transmitted in the clear.**

**(U) Controlling Network Access**

(U) Use network intrusion detection systems as an early warning for unauthorized access attempts. Always use secure routers and firewalls to filter traffic and block ports.

**(U) WARNING: Ports 135, 137, 138, and 139 should be blocked at the premise router.**

**(U) NOTE: Windows NT uses Ports 135, 137, 138, and 139 when NetBIOS over TCP/IP is enabled. Their functions are: Port 135 – (TCP) RPC location service, Port 137 – (UDP) NetBIOS name resolution request, Port 138 – (UDP) NetBIOS authentication, name registration, and browsing services, Port 139 – (TCP) NetBIOS Session for Server Message Blocks (SMBs) that perform file transfers and print jobs.**

## (U) Windows NT 4.0 Service Pack 4 Readme File

(U) This is the complete, formatted Windows NT 4.0 Service Pack Four Readme file from Microsoft. It is available at <http://www.microsoft.com>.

```
=====
Microsoft Windows NT 4.0 Workstation
and Windows NT 4.0 Server
Service Pack 4 (128-bit Version)
=====
```

(c) Copyright Microsoft Corporation, 1998

This document provides information about Microsoft Windows NT 4.0 Workstation and Windows NT 4.0 Server Service Pack 4 (SP4), as well as answers to questions that you might have.

```
-----
HOW TO USE THIS DOCUMENT
-----
```

To view Readme.txt on the screen in Notepad, maximize the Notepad window. For best viewing, click Edit, and then click Word Wrap.

To print Readme.txt, open it in Notepad or another word processor, click the File menu, and then click Print. For best printing results, click Edit, click Set Font, type 9 in the Size box, and then click OK.

For a current list of computer and hardware peripherals supported by Windows NT 4.0, see the Windows NT Hardware Compatibility List at <http://www.microsoft.com/hwtest/hcl>.

```
=====
CONTENTS
=====
```

### 1.0 INTRODUCTION

- 1.1 What's New in Service Pack 4
- 1.2 Downloading and Extracting the Service Pack

### 2.0 INSTALLATION INSTRUCTIONS FOR WINDOWS NT 4.0 SERVICE PACK 4

- 2.1 Before You Install the Service Pack
- 2.2 Installing the Service Pack
- 2.3 Service Pack Uninstall
- 2.4 Year 2000 Service Pack Installation

### 3.0 USER NOTES

- 3.1 Emergency Repair Disk
- 3.2 Adding New Components to the System
- 3.3 Installing Symbol Files from the CD

# UNCLASSIFIED

- 3.4 Hardware Compatibility with Windows NT 4.0
  - 3.5 DIGITAL Alpha Notes
  - 3.6 Running Windows NT Administrative Tools from Remote Server
  - 3.7 CryptoAPI and Authenticode
  - 3.8 Uninstalling Internet Explorer
  - 3.9 Certificate Server Notes
  - 3.10 Internet Information Server 4.0, Secure Sockets Layer and Root CA Certificates
  - 3.11 Message Queue Notes
  - 3.12 Installing COM Internet Services
  - 3.13 Event Log Service
  - 3.14 Upgrading a Cluster to SP4
- 4.0 ADDITIONAL FIXES AND WORKAROUNDS
- 4.1 Installing Windows NT 4.0 on a Windows NT 5.0 Computer
  - 4.2 Dual Booting Between Versions of Windows NT 4.0 and Windows NT 5.0
  - 4.3 NTFS Version 4 and NTFS Version 5 Support
  - 4.4 Installing SP4 on a Windows NT Server Enterprise Edition System
  - 4.5 Internet Information Server 4.0
  - 4.6 Security Configuration Manager
  - 4.7 Updating Audio Drivers
  - 4.8 Microsoft Proxy Server
- 5.0 APPLICATION NOTES
- 5.1 CheckIt Diagnostic Kit 4.0 by Touchstone
  - 5.2 Norton CrashGuard 2.0 for Windows NT
  - 5.3 Inoculan 4.0
  - 5.4 Exceed
  - 5.5 Terminal Server
  - 5.6 Microsoft NetMeeting Y2K and Security Issues
  - 5.7 Numega SoftIce
  - 5.8 Microsoft BackOffice Small Business Server
  - 5.9 Rational Visual Quantify Version 4
  - 5.10 Microsoft IntelliPoint
- 6.0 LIST OF BUGS FIXED IN WINDOWS NT 4.0 SERVICE PACKS 1-4
- 7.0 DEPLOYMENT NOTE FOR SERVICE PACK 4 (128-BIT VERSION)
- 8.0 EXPORT RESTRICTIONS FOR SERVICE PACK 4 (128-BIT VERSION)
- 9.0 STRONG ENCRYPTION SUPPORT IN THIS SERVICE PACK 4 (128-BIT VERSION)

=====

## 1.0 INTRODUCTION

=====

This release of Microsoft Windows NT 4.0 Service Pack 4 (SP4) is easy to apply while Windows NT is running and updates all files that are older than those included in this Windows NT Service Pack. Service Pack releases are cumulative and contain all previous Service Pack fixes and any new fixes created after Service Pack 3.

IMPORTANT: It's recommended that you stop running any critical services before you apply Windows NT 4.0 SP4. For more preinstallation recommendations, see section 2.1, "Before You Install the Service Pack."

## 1.1 What's New in Service Pack 4

### 1.1.1 Active Accessibility Support

Microsoft Active Accessibility (MSAA) is a COM-based standard method by which a utility program interacts with an application's user interface (UI). Using MSAA applications can expose all UI elements and objects with standard properties and methods. SP4 includes five new application programming interfaces (APIs). These new APIs include:

- \* GetGUIThreadInfo
- \* GetAncestor
- \* RealChildWindowsFromPoint
- \* RealGetWindowClassA
- \* RealGetWindowClassW

### 1.1.2 DCOM/HTTP Tunneling

This update allows DCOM client/server communication to cross firewalls over the HTTP protocol port. The new protocol "Tunneling TCP" is used like other DCOM protocols. The new moniker type OBJREF is passed in HTML to the client. The benefits of Tunneling TCP include high performance, use of existing open ports in the firewall, and control of client access for proxy administrators. For more information, see <http://www.microsoft.com/com>.

For instructions on installing Tunneling TCP, see section 3.11, "Installing COM Internet Services" under User Notes.

### 1.1.3 Euro Key Patch

The Euro Key Patch is an update to include the new European "euro" currency symbol. The update supplies the core fonts (Arial, Courier New, and Times New Roman) and the keyboard drivers.

### 1.1.4 InternetGroup Management Protocol (IGMP) v2

IGMPv2 allows a computer to inform the router that it's leaving a group. This update enables the router to determine if there are no more members in a group and then executes a command to stop forwarding mcast packets on to the link. This update is useful when users are frequently joining and leaving groups.

### 1.1.5 Microsoft File and Print Service for NetWare (FPNW) Support for Client32

Microsoft File and Print Services for NetWare permits the Windows NT 4.0 Server to act as a NetWare 3.X Server and is able to process file and print requests from NetWare clients without changing or updating the NetWare client software. This Service Pack provides an update that allows Windows NT 4.0 to support NetWare's Client32. This update installs only on those computers that have the FPNW service already installed.

### 1.1.6 Proquota.exe

The Proquota.exe is a utility that can be set up to monitor the size of users' profiles. If an individual user's profile exceeds the

predetermined file limit, the user won't be able to log off of the computer until the user reduces the size of the file.

## 1.1.7 Remote Winsock (DNS/Port 53)

Proxies or firewalls will often disable the Domain Name System (DNS) port number 53 in order to deter external sites from querying the internal DNS structure. As a result, inbound response packets sent on port 53 can't be received. SP4 provides a solution to change the Windows NT DNS server port number and configure it to use a different port number when connecting outbound.

To enable this feature, a registry value "DWORD" is created. Locate `\services\dns\parameters\SendOnNonDnsPort` and set to a non-zero value to go off port 53. If the value is < 1024 the server can use any port number. If the value is > 1024 the server will use the port number specified.

## 1.1.8 Remote Procedure Calls (RPC) Enhancements for Visual Basic (VB)

RPC enhancements for VB have been provided in this release. In VB, a "User Data Type (UDT)" is added allowing the TypeLib arrangement of structures. These new user interfaces, IRecordInfo, provide UDT information and a UDT field for the Access Database.

## 1.1.9 Routing Information Protocol (RIP) Listener

If you utilize RIP Listener on a computer running Windows NT 4.0, you can use SP4 to update this component. If you want to install RIP Listener after you apply SP4, use the following procedure.

>>>To install the RIP Listener:

1. Insert the SP4 CD into the disc drive, and change the folder to `\I386` (or `\Alpha`).
2. Copy `Oemnsvir.wks` to `D:\<winntsystemroot>\system32\oemnsvir.inf`.
3. Click Start, point to Settings, and click Control Panel. Double-click Network, and on the Services tab, click Add.
4. In Network Service, select RIP for Internet Protocol, and then click OK.
5. In the Windows NT Setup dialog box, type the path for the location of the SP4 files and click OK.

## 1.1.10 Visual Studio-MICS

This Service Pack includes an update to Visual Studio called Visual Studio Analyzer Events. Visual Studio Analyzer Events provides a graphical representation of high-level behaviors and their solutions. Use Visual Studio Analyzer Events to view graphically simple tables of event logs, the system's performance, and Windows NT Performance Monitor (NT PerfMon), as well as other system data.

## 1.1.11 Year 2000 (Y2K) Fixes

This Service Pack contains fixes for known Year 2000 issues for Windows NT 4.0, including:

- \* The User Manager and User Manager for Domains recognize the year 2000 as a leap year.
- \* The Date/Time Control Panel applet can update the system clock.
- \* Find Files supports only numeric character recognition in the decades field.
- \* Word document properties recognize both 1900 and 2000 as valid

centuries and support four-digit years.

\* The Dynamic Host Configuration Protocol (DHCP) administrators program supports displaying the years between 2000-2009 with a minimum of two digits.

For more information, see section 2.4, "Year 2000 Service Pack Installation."

#### 1.1.12 Compaq Fiber Storage Driver

This driver and .Inf are located in the \Drvlib folder. When installed, the Compaq fiber storage driver along with the .Inf provides support for Compaq fiber storage devices. The certified devices are:

\* Compaq Fiber Channel Host Controller/P for PCI.

\* Compaq Fiber Channel Host Controller/E for EISA.

#### 1.1.13 Internet Explorer 4.01 Service Pack 1

Internet Explorer 4.01 Service Pack 1 is located in SP4 in the \Msie401 folder. Run ie4setup.exe to install this version of Internet Explorer on your computer.

#### 1.1.14 Message Queue (MSMQ) for Windows 95 Client

This Service Pack also includes MSMQ Windows 95 Client fixes, located in the \Support\Msmq.95 folder. Most problems that are mentioned in section 3.10, "Message Queue (MSMQ) Notes," also apply to Windows 95. In addition, the Windows 95 MSMQ update fixes a problem causing long delays with MQOpenQueue() and MQIS operations on offline computers. This MSMQ Windows 95 update doesn't have an uninstall option.

#### 1.1.15 Option Pack Fixes

This Service Pack release includes Option Pack fixes and enhancements. If you have the Internet Information Server version 4.0 Option Pack installed, the Service Pack 4 update program will automatically update the Option Pack components installed on your computer.

When beginning the installation of the Windows NT Option Pack 4.0 on a server with Windows NT SP 4.0 and Internet Information Server 3.0, the following message may appear:

"Setup detected that Windows NT 4.0 SP4 or greater is installed on your machine. We haven't tested this product on SP4. Do you wish to proceed?"

The Windows NT Option Pack 4.0 is fully tested and supported to run on servers with the Windows NT Service Pack 4.0. Click Yes to continue Setup.

NOTE: It's recommended that you reinstall SP4 after you install Windows NT Option Pack 4.0. Otherwise, an MSMQ MQIS Controller installation won't work until the Windows NT Service Pack 4.0 is reinstalled.

##### 1.1.15.1 Certificate Server

The Microsoft Certificate Server is a standards-based, highly customizable server application for managing the creation, issuance, and renewal of digital certificates. Certificate Server generates certificates in standard X.509 format. These certificates are used for a number of public-key security and authentication applications including, but not limited to, server and client authentication under the Secure Sockets

# UNCLASSIFIED

Layer (SSL) protocol and secure e-mail using Secure/Multipurpose Internet Mail.

The update to Certificate Server includes:

- \* Teletex Encoding--Data encoded as teletex in a certificate request will be encoded as teletex data in the certificate issued. Formerly, this data would have been encoded as Unicode in the certificate issued.
- \* Serial Number--Serial numbers are generated according to X.509 standards. These serial numbers are automatically generated, unique, and always positive. This is to accommodate restrictive mail clients.
- \* Backup/Restore--Specific backup requests are supported, including backing up keys and certificates.
- \* An update to the default policy module so that mail certificates issued are usable by Outlook 98.
- \* An update to Certificate Server to fix a problem with certificates issued on February 29th of a leap year. Previously, the validity period would have the NotBefore and NotAfter dates set to the same date. With this update, NotBefore and NotAfter are now set correctly in the context of the CA validity for certificates issued on February 29th of a leap year.

For information on how to use the keys and certificate backup/restore utility, go to the Knowledge Base at <http://support.microsoft.com/support/> and search for KB article Q185195.

This release of Certificate Server doesn't support certificate hierarchies. However, a limited subset of the functions of Certificate hierarchies work specifically with Exchange.

You can get additional information on this from a white paper titled "Creating Certificate Hierarchies with Microsoft Certificate Server Version 1.0." This is available as a self-extracting .exe file (Hier3.exe) on the Microsoft Web site at <http://support.microsoft.com/support/downloads/LNP279.asp>.

## 1.1.15.2 Index Server

Index Server is a content indexing engine that provides full text retrieval for Web sites. Index Server requires that Internet Information Server be installed.

## 1.1.15.3 Internet Information Server (IIS)

The following Internet Information Server version 4.0 Option Pack components are installed on your computer:

1. Security Enhancements--Support for long file names for access restrictions on a file or a folder.
2. Performance--Improvements on the logging and caching of information. These improvements include, but aren't limited to:
  - \* IIS 4.0 performance on extension mapping.
  - \* IIS 4.0 memory performance for mapping log files.
  - \* IIS 4.0 performance in mapping unmapped data files if memory configuration is low or stressed.

## 1.1.15.4 Message Queue (MSMQ) for Windows NT

This update to MSMQ includes:

- \* Performs cleanup of unused message file space every six hours to reduce disk-space usage.  
NOTE: This schedule may be configured via the <MessageCleanupInterval> MSMQ registry key (in milliseconds).
- \* Clears all obsolete express message files when the MSMQ service starts.
- \* Enforces case insensitivity with foreign language characters in private queue names.
- \* Reduces occurrences of duplicate messages in persistent delivery mode.
- \* Exhibits performance counters for remote queues after a system recovery.
- \* Correctly shows per-session outgoing messages performance counters.
- \* MSMQ MQIS servers refresh cached information every 12 hours.
- \* Fixes a problem causing transactional messages to be rejected in some cases.
- \* Allows specifying external certificates via the MSMQ ActiveX components interface.
- \* Transactional messages can be read from connector queues after restarting the MSMQ connector application.
- \* MQSetQueueSecurity for private queue is supported.
- \* MQCreateQueue for private queues now works on Windows NT Server 4.0 Option Pack installations on Microsoft Cluster Server computers.
- \* Supports sending Microsoft PowerPoint and Microsoft Word documents using ActiveX components.
- \* Fails when user attempts the renewal of internal certificates when Primary Enterprise Controller (PEC) is unreachable.
- \* Machine quota limitation correctly recomputed after restarting the MSMQ service.
- \* MSMQ COM objects correctly process asynchronous message arrival events in multithreaded applications.
- \* Improved detection and reporting of corrupted message packets in message files that could have resulted in a hung MSMQ service previously.
- \* Transactional messages sent offline are no longer rejected with a bad message class: MQMSG\_CLASS\_NACK\_BAD\_DST\_Q. The symptom was that such messages were immediately routed to the sender's exact dead letter queue.
- \* Supports sending messages to different computers that have the same IP address. This can happen when a server attempts to send messages to two different RAS clients that happen to be assigned the same address one after the other.
- \* Recovers correctly when sending messages from a server to a client whose address is no longer valid (e.g., a RAS client that has timed-out). Previously, extra message traffic might have been generated.
- \* Asynchronous messaging now functions correctly on Japanese Windows 95 when using the MSMQ COM objects.
- \* Fixes a problem in the MSMQ COM objects when referencing the response and admin queue properties of a message for queues not explicitly refreshed from the MQIS.

## UNCLASSIFIED

- \* In Windows 95, calling MQOpenQueue with a DIRECT format no longer blocks for a long time.
- \* If the Windows NT 4.0 licensing service isn't running, then MSMQ per-seat licensing is no longer enforced.
- \* A specific call to MQLocateBegin no longer causes an exception on the MQIS server. This could have occurred previously when the Label restriction specified with an incorrect vt argument (anything other than VT\_LPWSTR).
- \* MSMQ applications can be run by users logged on to local machine accounts. Note that this used to work anyway for shadowed local accounts -- i.e., for accounts that had "identical" local accounts (user name/password) on the server machine. The default security for queues created by such users is that everyone is granted full control (in particular, read and delete permissions).
- \* A new MQIS update/restore utility is supplied that enables administrators to seamlessly recover crashed MQIS servers. See support\msmq.nt\MQISwizard.doc for more information.

### 1.1.15.5 Microsoft Transaction Server (MTS)

MTS is updated with a new Java Context class. If you're building applications using Visual J++, you can use the new Context class instead of IObjectContext. The Context class allows you to do the following using Visual J++:

- \* Declare that the object's work is complete.
  - \* Prevent a transaction from being processed, either temporarily or permanently.
  - \* Instantiate other MTS objects and include their work within the scope of the current object's transaction.
  - \* Determine whether a caller is in a particular role.
  - \* Determine whether security is enabled.
  - \* Determine whether the object is executing within a transaction.
- See the Visual J++ section of the Programmer's Reference for complete documentation of the new class.

### 1.1.15.6 SMTP, NNTP

Simple Mail Transport Protocol (SMTP), Network News Transport Protocol (NNTP) enhancements are available in this Service Pack. SMTP now supports the following services:

- \* Multiple virtual servers, or sites.
- \* ETRN command for dequeuing mail over dial-up connections.

>>>To enable this functionality:

1. Create a text file with the following text:

```
set obj = GetObject ( "IIS://localhost/smtpsvc" )
obj.Put "SmtpServiceVersion", 2
obj.SetInfo
```

NOTE: This is an Active Directory Service Interface (ADSI) script that will update a value in the metabase.

2. Save this file as Enable.vbs.

3. From a command prompt, type the following and press ENTER:

cscript enable.vbs

For more information, go to the Knowledge Base at <http://support.microsoft.com/support/> and search for KB article Q183476.

You can also point to specific KB articles using the following example:  
<http://support.microsoft.com/support/kb/articles/Q151/8/60.asp>

#### 1.1.16 Security Configuration Manager (SCM)

Security Configuration Manager (SCM) is an integrated security system that gives administrators the ability to define and apply security configurations for Windows NT Workstation and Windows NT Server installations. SCM also has the capability to perform inspections of the installed systems to locate any degradation in the system's security. For further information on SCM, including installation and usage instructions, refer to *Readme.txt* in the *\Mssce* folder.

#### 1.1.17 Web-based Enterprise Management (WBEM)

WBEM/WMI is Microsoft's implementation of Web-Based Enterprise Management (WBEM), the new standard for representation of management information as supported by the Desktop Management Task Force. It surfaces important management data from Windows NT and makes it freely available to any management tool through a number of well-defined interfaces so that management of Windows NT becomes much easier (included on CD-ROM only). For more information on WMI, see <http://www.microsoft.com/management/wbem>.

WBEM consolidates and unifies the data provided by existing management technologies. WBEM focuses on solving real enterprise issues by tracking problem areas from the user/application level through the systems and network layers to remote service/server instances. For more information, see <http://wbem.freerange.com/>.

You can download the Web-Based Enterprise Management Software Developer's Kit (SDK) at <http://msdn.microsoft.com/developer/sdk/wbem/sdk/default.htm>.

#### 1.1.18 Microsoft Windows NT Server NetShow Services

SP4 contains an updated version of NetShow Services located on this CD in the *\NetShow* folder. NetShow Services enables Internet service providers (ISPs) and organizations to deliver the highest-quality audio and video at every bandwidth across the Internet or enterprise networks. This release of NetShow Services features greatly enhanced audio and video that delivers the best user experience. Simplified setup, configuration, and administration of the NetShow server components and tools give ISPs a reliable and cost-effective platform for hosting large amounts of content.

Consult the NetShow Services information page (*\NetShow\ntsp4-ns.htm*) for details on installing and configuring this product. Before installing this product, you should also carefully review the NetShow Services release notes at *\NetShow\ns-readme.htm*.

#### 1.1.19 Microsoft Windows Media Player

Microsoft Windows Media Player replaces Microsoft ActiveMovie as well

as the Microsoft NetShow Player. Windows Media Player has all the features found in both of the other multimedia players, plus many more. It also upgrades existing Windows Media Player and ActiveMovie support to provide convenient access to new Windows Media content. Windows Media Player supports most local and streaming multimedia file types including WAV, AVI, QuickTime, RealAudio 4.0 and RealVideo 4.0. The new player takes over the class IDs of the previous players. After you install the new player, programs that used the old class IDs will function as usual. Windows Media Player is located in the \Mplayer2 folder on the compact disc.

1.1.20 Security Privilege Must Be Enabled to View Security Event Log  
SP4 includes a bug fix in the Event Log service that requires that the SE\_SECURITY\_NAME privilege, also known as the Security privilege, be enabled in order to view and manage the security event log. By default, Windows NT grants the privilege to administrators and local System. In order to take effect however, the privilege must also be enabled in the program accessing the security event log.

Prior to this change, members of the Administrators group and services running as local System could open the security log for read or change access without enabling the Security privilege. If the privilege was removed from the Administrators group, members of the Administrators group could still manage the security log. This change enforces the security model that administrators need to be granted the privilege to manage the security log; they won't be able to manage the log simply because they are members of the Administrators group. Administrators can always grant themselves the Security privilege to manage the security log, however, although this event can be audited.

For more information, consult the Knowledge Base at <http://support.microsoft.com/support/> and search for KB article Q188855.

1.1.21 Dynamic Host Configuration Protocol (DHCP)  
This Service Pack includes several quality improvement fixes to correct known Dynamic Host Configuration Protocol (DHCP) issues reported for Microsoft DHCP Server, the DHCP Manager administration tool, and for Microsoft DHCP-enabled clients running under earlier released versions of Windows NT 4.0.

These fixes address specific problems fully described in the Q184693 "DHCP/WINS Release Notes for Windows NT 4.0 SP4 Update" article in the Knowledge Base:

You can obtain the specific article from Microsoft Support Online at <http://support.microsoft.com/support>.

1.1.22 Windows Internet Naming Service (WINS)  
Windows NT Server includes the following new Windows Internet Naming Service (WINS) and WINS Manager features:

- \* Manual removal of dynamic WINS database records.
- \* Multi-select operations for WINS database records.
- \* Burst mode handling for WINS servers.

1.1.23 Microsoft Routing and Remote Access Service (RRAS)  
SP4 can now be installed on a Windows NT 4.0 system running Routing

and Remote Access Service (RRAS). SP4 will update your RRAS system to RRAS Hotfix 3.0 components automatically. If you install RRAS after installing SP4, you must reinstall SP4 to get the updated RRAS files to ensure RRAS will work properly. For more information on RRAS Hotfix 3.0, see <http://support.microsoft.com/support/kb/articles/Q189/5/94.asp>.

#### 1.1.24 PPTP Performance and Security Update

SP4 now includes new performance and security updates to PPTP that greatly increase data transfer speeds and enhance security. The PPTP client and server system must both be running the updated files to get the new benefits. For more information, see <http://support.microsoft.com/support/kb/articles/q189/5/95.asp>

#### 1.1.25 NTLMv2 Security

SP4 contains an enhancement to NTLM security protocols called NTLMv2, which significantly improves both the authentication and session security mechanisms of NTLM. For more information, see <http://support.microsoft.com/support/kb/articles/q147/7/06.asp>.

#### 1.1.26 Secure Channel Enhancements

SP4 contains an enhancement to the secure channel protocols used by member workstations and servers to communicate with their domain controllers and by domain controllers to communicate with other domain controllers. In addition to authentication, you can now encrypt and check the integrity of these communications. For more information, see <http://support.microsoft.com/support/kb/articles/q183/8/59.asp>

#### 1.1.27 IP Helper API (IPHLPAPI)

The IP Helper API provides Windows network configuration and statistics information to Win32 applications. The public API is available on Windows NT 4.0 and above, and Windows 95 and above. SP4 updates the API with a new .dll so that applications can communicate to a TCP/IP stack.

#### 1.1.28 Event Log Service

This Service Pack contains new features in the Event Log Service to assist how administrators measure the reliability and availability of Windows NT.

The SP4 Event Log Service records three new events in the system event log that are useful in measuring operating system availability:

- \* Clean Shutdown Event (Event ID: 6006)
- \* Dirty Shutdown Event (Event ID: 6008)
- \* System Version Event (Event ID: 6009)

See section 3.12, "Event Log Service," for more information.

#### 1.1.29 Domain Name Server (DNS) Service

This Service Pack includes several quality improvement fixes to correct known Domain Name Server (DNS) issues reported for Microsoft DNS Server and the DNS Manager administration tool. These fixes address specific problems described in the Q184693 "DNS/DHCP/WINS Release Notes for Windows NT 4.0 SP4 Update" article in the Knowledge Base. You can obtain the specific article from Microsoft Support Online at <http://support.microsoft.com/support>.

-----  
1.2 Downloading and Extracting the Service Pack  
-----

If you have downloaded this Service Pack from an FTP site or a Web site, you should read the release notes completely before you extract and install the Service Pack. For this release, these self-extracting executables are also located at the root of the CD. They are Sp4alpha.exe for Alpha processor type systems and sp4i386 for Intel-based systems.

After downloading the Service Pack, you'll have a compressed executable file on your hard drive. To extract this file and begin the installation process, for example, type Sp4i386.exe at the command prompt or double-click the file from Windows NT Explorer. You can also extract the file into the current folder without launching the installation program by using the command prompt switch /x (for example, at the command prompt, type sp4i386 /x).

=====  
2.0 INSTALLATION INSTRUCTIONS FOR WINDOWS NT 4.0 SERVICE PACK 4  
=====

Carefully read the installation instructions before you install Service Pack 4, as they may have changed from previous Service Packs.

-----  
2.1 Before You Install the Service Pack  
-----

Close all active debugging sessions before installing this Service Pack, otherwise the Update program will be unable to replace system files that are in use. If a file is in use when you install the Service Pack, a dialog box will appear in which you can choose to cancel the installation or skip the file copy. It's recommended you choose to cancel the installation, and then uninstall SP4. To do this, run Spuninst.exe or click Start, point to Settings, click Control Panel, double-click Add/Remove Programs, and then click Uninstall Service Pack 4. Close all active sessions on the system, and then run Update.exe again to install the Service Pack.

Also, to maximize the ability to recover the system in the event of installation failure, it's recommended that you do the following before installing the Service Pack:

1. Update the system Emergency Repair Disk using the Rdisk.exe command with the /s switch.
2. Perform a full backup of the system, including the system registry files.
3. Disable any nonessential third-party drivers and services (that is, drivers and services that aren't required to boot the system).
4. Contact the original equipment manufacturer (OEM) that provided the driver or service for the updated versions of the file(s).
5. Restart the computer and check Event Viewer to ensure there are no system problems that could interfere with the installation of SP4.

Users of NEC Versa 6050 or 6200 Series notebook computers, with

# UNCLASSIFIED

Windows NT version 4.0 preinstalled, should select "Yes" when SP4 Update.exe prompts you to replace the hal.dll file.

If your computer contains SystemSoft Card Wizard version 2.x or earlier, you must obtain SystemSoft Card Wizard version 3.00.01 or greater before installing Windows NT 4.0 Service Pack 4. Otherwise, your operating system will no longer function. Contact SystemSoft at <http://www.systemsoft.com> for further details.

Advanced Power Management isn't supported by Windows NT 4.0. As a result, it's recommended that you remove Advanced Power Management features before installing this Service Pack.

Power Management Utilities may not work on Windows NT 4.0 Service Pack 4. Contact the vendor of your Power Management Utilities for an updated version to work with Windows NT 4.0 SP4.

Do not install SP4 without the Silicon Graphics companion software. SP4 requires additional files to update your Silicon Graphics system. For these necessary files, visit the Silicon Graphics Web site at <http://support.sgi.com/nt>.

## ----- 2.2 Installing the Service Pack -----

>>>To install the Service Pack from the CD

1. Insert the Service Pack CD into your CD-ROM drive.
2. If a Web page opens in your browser after you insert the CD, click Windows NT Service Pack, and then click Install Service Pack.
3. When you're asked whether you want to open the file Spsetup.bat or save it to disk, click Open and then follow the instructions that appear on the screen.

NOTE: To use the uninstall feature of this Service Pack, you must create an Uninstall folder during the initial installation.

4. If a Web page doesn't automatically open when you insert the CD, open the Command Prompt window and change the folder to the drive letter associated with the CD-ROM drive.
5. Change the folder to \I386\Update or \Alpha\Update (depending upon whether you have an x86 or Alpha CPU), and type UPDATE.
6. Follow the instructions that appear on the screen.

If SP4 doesn't install after you click Install Service Pack 4 from the CD, or your browser doesn't automatically display installation instructions when you insert the CD into your CD-ROM drive, start the Service Pack install process manually from the CD. For more information, see "To install the Service Pack from the CD" mentioned earlier in this section.

NOTE: To use the uninstall feature of this Service Pack, you must create an Uninstall folder during the initial installation.

>>>To install the Service Pack from a network drive

1. Run the command to connect to the network drive that has the Service Pack files.

# UNCLASSIFIED

2. Change the drive letter to that network drive.
3. Change the folder to \I386\Update or \Alpha\Update (depending upon whether you have an x86 or Alpha CPU), and then type UPDATE.
4. Follow the instructions that appear on the screen.

NOTE: It's recommended that you choose to create an Uninstall folder the first time you install the Service Pack.

>>>To install the Service Pack from the Internet Using a Web browser (such as Internet Explorer 3.0 or later), visit <http://support.microsoft.com/support/ntserver/content/servicepacks/> or <http://support.microsoft.com/support/downloads/>. Click the Install Service Pack 4 option to install SP4 on your computer. This Web page automatically detects which files need to be updated and then copies the appropriate files to a temporary folder on your computer. It then installs only those files that are needed to update your computer.

NOTE: If you use Web browsers other than Internet Explorer 3.0 or later, you may be unable to install the Service Pack through this update method. If you are unable to install the Service Pack using this option, download the entire Service Pack from the Internet onto your computer and run update.exe locally.

There are installation switches that can be used with Update.exe. The following syntax help is available by typing update /?:

```
UPDATE [-u] [-f] [-n] [-o] [-z] [-q]
-u Unattended mode
-f Forces other apps to close at shutdown
-n Do not back up files for uninstall
-o Overwrite OEM files without prompting
-z Do not reboot when installation is complete
-q Quiet mode - no user interaction
```

## ----- 2.3 Service Pack Uninstall -----

This Service Pack contains an uninstall feature that you can use to restore your system to its previous state.

To enable the uninstall option, run Update.exe. A subfolder in your Windows NT folder named Uninstall will be created. This requires at least 80 megabytes (MB) of free space on the drive on which Windows NT is installed. This is 40 MB for the uninstall folder and 40 MB for the Service Pack updated system files.

To uninstall SP4, double-click the Add/Remove Programs control panel. Select Windows NT 4.0 Service Pack 4, and click Add/Remove. If this option isn't available, run Spuninst.exe from the %systemroot%\\$NtServicePackUninstall\$\spuninst\ folder.

NOTE: If you install any applications or services that require SP4 or have bug fixes contained in SP4, uninstalling SP4 could adversely affect those applications.

If you want to uninstall SP4, the drive letter for the boot drive must

be the same as when you installed SP4. If you change the drive letter for the boot drive, you can't uninstall SP4.

To uninstall Service Pack 2 and Service Pack 3, you had to run Update.exe and then select "Uninstall a previously installed Service Pack." This returned your system to its previous state. After your system restarted, the Update.exe program replaced the files updated by the Service Pack with most of the files from the previous installation and returned most of your registry settings to what they were before that Service Pack was installed.

NOTE: If you uninstall SP4 on a system that previously had Service Pack 3 (without Internet Explorer 4.0) installed on it, cryptography won't work correctly after the uninstall completes. To work around this issue, reinstall Service Pack 3 after you have uninstalled SP4.

Uninstalling SP4 won't uninstall new versions of CryptoAPI and SChannel.

NOTE: If you plan to install a previous Service Pack after uninstalling SP4, take note of the following important precaution. SP4 modifies the Security Account Manager (SAM) database and the Security database such that older versions of the Samsrv.dll, Samlib.dll, Lsasrv.dll, Services.exe, Msv1\_0.dll and Winlogon.exe files no longer recognize the database structure. Therefore, the uninstall process doesn't restore these files when uninstalling SP4. If you install a prior Service Pack (for example, Service Pack 3) after uninstalling SP4, click "No" on the "Confirm File Replace" dialog boxes that ask if you want to overwrite Samsrv.dll and Winlogon.exe. If you overwrite the newer files with these older versions, you'll be unable to log on to the system.

NOTE: If you're reinstalling SP4 after installing new software or hardware, you must choose to create a new Uninstall folder. To retain your ability to back out to a bootable configuration, copy the current Uninstall folder to a safe location before running the SP4 installation program.

-----  
2.4 Year 2000 Service Pack Installation  
-----

Windows NT Service Pack 4 contains fixes for known Year 2000 issues in the Windows NT 4.0 operating system.

>>>To install the Year 2000 Service Pack from compact disc

Installing the Service Pack using Update.exe will update all necessary files on your Windows NT 4.0 installation. It will also detect and inform you if any additional Microsoft components that require updating to resolve known Year 2000 issues in the Windows NT 4.0 operating system. Follow the procedure below to update your computer to resolve known Year 2000 issues.

Run the Y2ksetup.exe program located in the \i386\Update (for x86-based computers) or \Alpha\Update (for Alpha-based computers) folders on the Service Pack 4 compact disc. This program automatically updates operating system components as detected to resolve known Year 2000 issues.

## UNCLASSIFIED

Note that this installation will require the system to be restarted one or more times. There is no uninstall option available for Y2ksetup.exe.

>>>To install the Year 2000 Service Pack via the Web or FTP

Install the base Service Pack from one of the locations below to your computer:

<http://support.microsoft.com/support/ntserver/content/servicepacks/>  
<http://support.microsoft.com/support/downloads/>

The download program will automatically detect which files need to be updated. Once prompted with the File Download dialog, select "Run this program from its current location" to perform a patched installation. This will also detect and inform you if any additional Microsoft components require updating to resolve known Year 2000 issues on your Windows NT 4.0 operating system. Follow the procedure below to resolve known Year 2000 issues.

Download the Year 2000 Service Pack (y2ksp4i.exe or y2ksp4a.exe) from one of the locations below to your computer:

<ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/>  
<http://support.microsoft.com/support/ntserver/content/servicepacks/>  
<http://support.microsoft.com/support/downloads/>

Run the self-extracting executable to expand the package. Run Y2ksetup.exe from \i386\Update (for x86-based computers) or \Alpha\Update (for Alpha-based computers) folder at the target location. This program automatically updates operating system components as detected to resolve known Year 2000 issues.

Note that this installation will require the system to be restarted one or more times. There is no uninstall option available for Y2ksetup.exe.

>>>If you need to reinstall this Service Pack, run Update.exe from the \i386\Update or \Alpha\Update folders. It isn't necessary to uninstall the Service Pack previous to running Update.exe more than once on the same system. Use \i386\Update\Y2ksetup.exe or \Alpha\Update\Y2ksetup.exe to resolve known Year 2000 issues in the Windows NT 4.0 operating system.

There are installation switches that can be used with Y2ksetup.exe. The following switches are available:

Y2KSETUP [-q] [-d]

-q silent mode installation

-d display only (does not install, only displays those operating system components on the computer that contain known Year 2000 issues)

### 2.4.2 Site Server Express 3.0

There are known Year 2000 issues in the following components of Site Server Express 2.0:

\* Content Analyzer

\* Usage Analyst

## UNCLASSIFIED

Installing Site Server Express 3.0 directly from the Web or from the CD doesn't remove these components from your computer. You must install Y2ksetup.exe to remove these components from your computer and install Site Server Express 3.0, which contains an update for:

- \* Usage Analyst
- \* Posting Acceptor

An updated version of the Content Analyzer will be available for download from the Windows NT Service Pack 4.0 Web site.

Known Site Server Express 3.0 setup issues:

- \* When Y2KSetup installs Internet Explorer 4.01 SP1 and Site Server Express 3.0, two IIS virtual roots that are required by Posting Acceptor aren't created. It's recommended that you reinstall Site Server Express 3.0 by running Ssx.exe from the \Ssx folder on the CD.

### 2.4.3 FrontPage Server Extension Year 2000 Issues

Releases of FrontPage 1.0, FrontPage 1.1 and FrontPage 97 are not Year 2000 compliant. Releases of FrontPage 98 resolve known Year 2000 issues. If you have NTOP installed, you will have FrontPage 98 Server Extensions. It's possible to have two or more versions of the FrontPage Server Extenders on your computer at one time. The installation of a version that isn't Year 2000 ready doesn't mean that you are actively running that version.

>>>To determine which version of the FrontPage Server Extenders are actively in use on computers with FrontPage 98 or earlier

- \* Run the FrontPage Server Administrator (Fpsrvwin.exe).
- \* Click on each of the Web servers or virtual servers listed in the box in the upper left area, which have been configured with the FrontPage Server Extenders.
- \* The version number of the FrontPage Server Extenders is displayed to the right of the list. Version numbers where the first digit is 3 or greater resolve known Year 2000 issues (e.g. 3.0.2.1706).

If the first digit of the version number is a 1 or 2, then you should download and install the latest version of the FrontPage Server Extenders. Refer to <http://www.microsoft.com/frontpage/> for details on the latest available version is and how to download.

### 2.4.4 IBM PS/1 ValuePoint

There are known Year 2000 issues for Windows NT version 4.0 on 2.4.4 IBM PS/1 ValuePoint computers. To fix these known issues, you must upgrade Ntdetect.com in order to resolve known Year 2000 issues in older versions.

From the \Ps1 folder on the CD, copy Ntdetect.com to the root of your primary boot partition on your computer. You do not need to reboot.

For more information, go to the Knowledge Base at <http://support.microsoft.com/support/> and search for KB article Q194301.

For Year 2000 issues regarding Microsoft products or definitions regarding Year 2000 compliance, as used herein, see our Web site at

<http://www.microsoft.com/year2000>.

=====

### 3.0 USER NOTES

=====

This section covers information that is specific to this Service Pack release.

-----

#### 3.1 Emergency Repair Disk

-----

If you use the Windows NT Emergency Repair Disk to repair your Windows NT system, which requires you to supply the original Windows NT media at some time after you install Service Pack 4, you'll need to reinstall SP4 after the repair is completed. This is because the Emergency Repair Disk repairs your system by restoring your original Windows NT 4.0 system files. After the repair is completed, follow the Installation Instructions (Section 2.0) to reinstall SP4. For more information on using the Windows NT Emergency Repair Disk utility, go to the Knowledge Base at <http://support.microsoft.com/support/> and search for KB article Q146887.

NOTE: To use the Emergency Repair Disk utility, you must have the updated version of Setupdd.sys. The updated version is contained in SP4. To update your version of Setupdd.sys, copy Setupdd.sys from the Service Pack to your Windows NT 4.0 Setup Disk 2 from the original product media. This will replace the older version of Setupdd.sys with the updated version. For more information, consult the Knowledge Base at <http://support.microsoft.com/support/> and search for KB article Q158423.

-----

#### 3.2 Adding New Components to the System

-----

If you change or add new software or hardware components to your system after you install SP4, you'll need to install the SP4 again. This is because the files included on the original Windows NT 4.0 media may not be the same as the files on the Service Pack CD. You can't install new components, such as a new keyboard or printer driver, directly from the Service Pack media. You must install new components from the original product media and then reinstall the Service Pack.

For example, if you install the Simple Network Management Protocol (SNMP) service after installing SP4, you'll need to reinstall the Service Pack. If you fail to do so, you'll receive the error message "Entrypoint SnmpSvcGetEnterpriseOID could not be located in Snmpapi.dll." This is because some of the files in the SNMP service have been updated in the SP4 and you have a version mismatch. Reinstalling the Service Pack fixes the problem by copying the newer versions of the files to your system.

NOTE: SNMP security provides the ability to set a permission level on the SNMP agent computer. The permission level determines how the SNMP agent computer will process requests from an SNMP community.

### 3.3 Installing Symbol Files from the CD

-----

Each program file in Windows NT has a corresponding symbol file that is used to find the cause of kernel STOP errors. The symbols for SP4 files are compressed in self-extracting executables named Sp4symi.exe and Sp4syma.exe, for Intel and Alpha respectively. To install the symbol files corresponding to the new binaries in SP4, run the executable and when prompted, specify the path to the location of the previous version's symbols (for example, c:\winnt\symbols\). This copies the SP4 .dbg files over the existing versions of these files.

For more information about debugging in Windows NT, see Chapter 39, "Windows NT Debugger," in the Microsoft Windows NT 4.0 Workstation Resource Kit.

-----

### 3.4 Hardware Compatibility with Windows NT 4.0

-----

#### 3.4.1 Video Drivers

Due to incompatibilities between the ATIRage drivers and Service Pack setup, the files Ati.sys and Ati.dll haven't been included with SP4. Any ATI drivers currently installed on your system will still function normally.

If you install SP4 over SP3 on a computer that has a Number Nine Visual Technologies Imagine 2 video card and drivers installed, you may experience some loss of functionality in the video driver, such as loss of any resolutions requiring 256 or more colors. If you uninstall SP4 and revert to SP3, the Imagine 2 card may be unable to display 256 colors or higher. There is no known resolution for either of these two issues because reinstalling the Imagine 2 video drivers doesn't restore the lost functionality. Number Nine is aware of this issue and is working on a fix.

#### 3.4.2 Dell Latitude Systems

If you're running Windows NT 4.0 on a Dell Latitude portable computer, your Dell-supplied Softex Advanced Power Management and PC Card Controller services (versions 2.0 and above) will continue to function after you install SP4. Softex version 1.0 will stop functioning after SP4 installation. To update your system for SP4, install version 2.19 or later of the Softex utilities, available from <http://support.dell.com/filelib/>. Your computer will become unusable if you reinstall any version of Softex prior to 2.19 after installing SP4.

#### 3.4.3 Softex/Phoenix Utilities

If you're using any of the following Softex Incorporated or Phoenix Technologies utilities, you may encounter problems running SP4:

- \* Softex PC Card Controller, or Phoenix CardExecutive for Windows NT
- \* Softex Power Management Controller, or Phoenix APM for Windows NT
- \* Softex Docking Controller, or Phoenix NoteDock for Windows NT
- \* Softex DeskPower Controller, or Phoenix DeskAPM for Windows NT

Follow these guidelines:

- 1) Obtain the version number of the utilities you're using.
- 2) You must be running version 2.19 or later of the Softex or Phoenix

# UNCLASSIFIED

utilities to avoid problems with SP4. Don't install or reinstall any version of Softex or Phoenix utilities earlier than 2.19 on your system, or your system might not boot. For more information, visit the Softex Incorporated Web site at <http://www.softexinc.com> or Phoenix Technologies at <http://www.phoenix.com>.

## 3.4.4 255 SCSI Logical Unit Support

Windows NT 4.0 detects only the first 8 logical units on a SCSI device. To work around this limitation, install SP4 and add the following key in the registry:

```
\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\[Driver Service Key]
\Parameters\Device[N]
    LargeLuns: REG_DWORD: 0x1
```

where [Driver Service Key] is your SCSI driver name and [N] is the SCSI bus number.

## 3.4.5 IBM PS/1 ValuePoint

There are known Year 2000 issues for Windows NT version 4.0 on this computer. It's necessary to upgrade Ntdetect.com in order to resolve known Year 2000 issues in older versions.

From the \Ps1 folder on the CD, copy Ntdetect.com to the root of your primary boot partition on your computer. You do not need to reboot.

For more information, go to the Knowledge Base at <http://support.microsoft.com/support/> and search for KB article Q194301.

## 3.4.6 SystemSoft Card Wizard

If your computer contains SystemSoft Card Wizard version 3.x and you have installed SP4, you may have lost socket services functionality. To work around this issue reinstall SystemSoft Card Wizard version 3.x or higher after installing Service Pack 4. Or you can copy Pcmcia.sys from the Service Pack 4 Uninstall folder, \$ntservicepacekuninstall\$, to the \%systemroot%\System32\Drivers folder on your computer. Reboot the computer.

## ----- 3.5 DIGITAL Alpha Notes -----

### 3.5.1 Using Remotely Possible 32 with Matrox Millennium Display Adapter

If you use Remotely Possible 32 on an Alpha with a Matrox Millennium display adapter, don't use the Matrox drivers. Otherwise, your computer bluescreens after rebooting. You must use VGA-compatible display adapter drivers to use Remotely Possible 32.

### 3.5.2 Lotus Notes 4.5

If you want to use Lotus Notes and Internet Explorer 4.01 on an Alpha computer that runs Windows NT 4.0, you must follow this sequence when installing SP4:

1. If you have Internet Explorer 4.01 on your computer, uninstall it.
2. Install SP4.
3. Install (or reinstall) Lotus Notes.
4. Install Internet Explorer 4.01 from the SP4 CD.

This problem will be fixed in a future release.

### 3.5.3 Alpha Fixes in SP4

These notes describe problems on Alpha systems that have been resolved since the Windows NT 4.0 Service Pack 3 release.

NOTE: Windows NT 4.0 SP4 ships with HAL Revision D. This revision is also currently available from Compaq.

#### 3.5.3.1 System Hangs on Alpha Systems with Only One Processor Physically Present

The following Alpha systems, with only one processor physically present, no longer hang when booted:

- AlphaServer 4x00
- AlphaServer 1200
- AlphaStation 1200
- DIGITAL Server 5000
- DIGITAL Server 7000

#### 3.5.3.2 Clock Interrupt Period Changed from 7.5 ms to 10 ms

In Windows NT 4.0 SP4, the effective clock interrupt period on the following systems was changed from 7.5 ms to 10 ms:

- AlphaServer 4x00
- AlphaServer 1200
- AlphaStation 1200
- DIGITAL Server 5000
- DIGITAL Server 7000

This change will provide parity with Intel systems and alleviate performance anomalies caused by assumptions of 10 ms for the resolution for timers (which is equal to the clock interrupt period).

#### 3.5.3.3 Pyxis Error Registers

HAL Revision D, which ships with Windows NT 4.0 SP4, supports updated Pyxis error registers, which provide more meaningful information during hardware crashes.

#### 3.5.3.4 Peer-to-Peer DMA Transfers

This Service Pack, together with the current AlphaBIOS firmware, now allows peer-to-peer DMA transfers.

#### 3.5.3.5 PCI Devices with 256 MB of Memory or Greater

The following Alpha platforms now support PCI devices with 256 MB of memory or greater for memory-mapped I/O:

- AlphaServer 1000 5/xxx
- AlphaServer 1000A 5/xxx
- AlphaServer 800 or Digital Server 3000
- AlphaStation 600
- AlphaStation 500
- Alpha XL 3xx

#### 3.5.3.6 Alpha Machines Sometimes Hang When Rebooting

The following systems no longer hang during an attempted reboot:

- AlphaServer 4x00
- AlphaServer 1200
- AlphaStation 1200
- DIGITAL Server 5000

DIGITAL Server 7000

3.5.3.7 I/O Performance Degradation or a Hung Machine Under Heavy I/O Loads On Alpha machines with heavy I/O loads, certain device drivers consumed too many DMA map registers. This sometimes caused poor I/O performance or a hung machine. SP4 allows a greater number of DMA map registers.

3.5.3.8 Crashes on Alpha systems with STOP Code 0x0A

Minor "correctable" hardware errors no longer generate crashes with STOP code 0x0A on following machines:

- AlphaServer 1000 5/xxx
- AlphaServer 1000A 5/xxx
- AlphaServer 800 or Digital Server 3000
- AlphaStation 600
- AlphaStation 500
- AlphaStation 600A
- Alpha XL 3xx

3.5.4 DIGITAL Ultimate Workstation 533

SP4 won't update the Hal.dll file on the system because Hal.dll is marked as an OEM file. To work around this, you must manually copy Halrawmp.dll from SP4 to your system. To do this, first locate the Hal.dll file on the system (in the OSLOADER subfolder), and then copy Halrawmp.dll from SP4 to this folder, renaming it Hal.dll.

3.5.5 Installation Fails on Alpha Machines with Windows NT Option Pack 1.0 Installed

Security Configuration Manager (SCM) doesn't install on Alpha machines that have the Windows NT Option Pack 1.0 for Alpha installed. This is because the Mfc42u.dll file installed by the Windows NT Option Pack isn't compatible with SCM.

To work around this, replace Mfc42u.dll installed by Windows NT Option Pack 1.0 for Alpha with Mfc42u.dll from the Windows NT4.0 CD or from Visual C 6.0. This may cause problems with the applications in the Windows NT Option Pack 1.0 for Alpha. This will be fixed in the next release of Windows NT.

3.5.4 Microsoft Transaction Server and Distributed Transaction Coordinator

The file TestOracleXAConfig.exe isn't automatically installed on DEC Alpha-based computers. If you are installing Windows NT 4.0 SP4 on an Alpha-based computer and will be using Microsoft Transaction Server (MTS) or the Distributed Transaction Coordinator (DTC) with an Oracle or XA-compliant database, you must manually copy this file from the CD-ROM to the %sysroot%\system32 folder on your hard drive. The symbol %sysroot% represents the installation folder for Windows NT. For example, if your installation folder is C:\Winnt, you would copy it to C:\Winnt\System32.

TestOracleXAConfig.exe is located in the \Alpha folder on the Windows NT 4.0 SP4 CD-ROM.

If you are installing Windows NT 4.0 SP4 on an Intel-based computer, TestOracleXAConfig.exe is automatically installed during Setup.

-----

## 3.6 Running Windows NT Administrative Tools from Remote Server

-----

In order to run administrative tools from a remote server, you must upgrade the remote server to Service Pack 4. If you attempt to run administrative tools from a remote machine that hasn't also been upgraded to Service Pack 4, they will fail to load or won't function properly.

-----

## 3.7 CryptoAPI and Authenticode

-----

The Authenticode environment won't be set up correctly for existing user accounts on upgrades from Windows NT 4.0 systems running Internet Explorer 3.02. This doesn't affect new user accounts created on the system. Also, upgrades from Windows NT 4.0 systems with Internet Explorer 4.0 or later aren't affected.

Each user needs to enter the following command line in a command prompt window before they use Authenticode:

```
setreg 1 false 2 true 3 false 4 false 5 true 6 false 7 true 8 false 9  
false 10 false
```

Setreg.exe isn't part of SP4; you can download it as part of the CryptoAPI tools. You can install the latest CryptoAPI tools (Internet Explorer 4.0 or later) from the Platform SDK on MSDN.

The CryptoAPI tools (also known as Authenticode Signing tools) that were released for Internet Explorer 3.02 are no longer supported. Tools released for Internet Explorer 4.0 will continue to work on Service Pack 4.

If you install SP4 on a system with Internet Explorer 4.0 or later and then uninstall Internet Explorer, newer CryptoAPI components will be partially uninstalled. This problem doesn't affect the system if Internet Explorer 4.0 was installed after SP4. Reinstall SP4 after uninstalling Internet Explorer for full functionality.

To ensure proper CryptoAPI functionality, it's recommended that you install Internet Explorer 3.02 or later before you install SP4. The following is a list of known problems when Internet Explorer 3.02 or later is installed after SP4:

- \* Certain CryptoAPI networking functions have a dependency on Wininet.dll and may fail if Wininet.dll isn't on the system. To work around this, install Internet Explorer 3.02 or later before installing SP4.

- \* Certificate revocation checking fails if you install Internet Explorer 4.0 after you install SP4. To fix this, reinstall SP4 after installing Internet Explorer 4.0. This will be fixed in a future release of Internet Explorer.

- \* Certain CryptoAPI-related file extensions (.Cer, .Crt, and .Der) aren't registered correctly when Internet Explorer 4.0 is installed after SP4. To restore the file extension registration, run the following command line:

```
Regsvr32.exe cryptext.dll
```

This will be fixed in a future release of Internet Explorer.

-----  
3.8 Uninstalling Internet Explorer  
-----

On a system that had Internet Explorer 4.0 or later installed and then had SP4 applied, uninstalling Internet Explorer will partially uninstall newer CryptoAPI components. Reinstall SP4 after uninstalling Internet Explorer. This problem doesn't affect the system if Internet Explorer was installed after SP4.

-----  
3.9 Certificate Server Notes  
-----

3.9.1 Known Problems and Limitations:

1. Be sure to consult the release notes for the Certificate Server version 1.0 as shipped with the Windows NT Option Pack. Also consult the QFE update release at <ftp://ftp.microsoft.com/bussys/iis/iis-public/fixes/usa/certserv>.
2. Do not perform an initial installation of Certificate Server on February 29th of a leap year. The validity period for the server will be set incorrectly. To work around this, set the machine time to the day before (February 28th), perform the installation, and then reset the machine time back to February 29th. There is no problem issuing certificates on February 29th, once the certificate server is successfully installed (as noted above).
3. If you install Certificate Server on top of SP4, you may receive a "Some system services could not start" error message upon system startup. Click OK to continue, and check the Event Viewer log for the specific error.

Event ID: 7000

Source: Service Control Manager

Description: The Certificate Authority service failed to start due to the following error: The service did not respond to the start or control request in a timely fashion.

Event ID: 7009

Source: Service Control Manager

Description: Timeout (120000 milliseconds) waiting for service to connect.

There are no workarounds for this problem.

3.9.2 Virtual Directory Attributes for Certificate Server

IIS enforces the application attribute of virtual directories in such a way that the Certificate Server's administration Web pages fail. This failure appears in the form of database access errors that are identified by an E78 access failure code. You will be unable to access the Certificate Server log and queue from the administration Web pages. To work around this problem, make sure that the application attribute for the Certificate Administration (CertAdm) folder is applied.

>>>To apply the application attribute for CertAdm folder:

1. Click Start, point to Programs, point to Windows NT 4.0

- Option Pack, point to Microsoft Internet Information Server, and then click Internet Service Manager.
2. In MMC, open the left pane entries until the Default Web Site is visible.
  3. Double-click the Default Web Site. The right pane now contains the first level of virtual directories for the Web server.
  4. Right-click the CertAdm virtual directory.
  5. Click Properties.
  6. In the Application Settings section of the Virtual Directory tab, click Create.
  7. Click Apply, and then click OK.

### 3.9.3 Invalid Hash Algorithm Accepted on Installation

During Certificate Server installation, don't select HMAC as the hash algorithm the Certificate Server should use when issuing certificates. Although HMAC is among the selections on the optional Advanced Settings page, this isn't a valid use of this algorithm. If HMAC is selected, installation of the Certificate Server will fail.

For more information about Certificate Server, consult the Microsoft Knowledge Base.

-----

### 3.10 Internet Information Server 4.0, Secure Sockets Layer and Root Certifying Authority Certificates, and the IISCA.EXE Tool

-----

If you use Internet Information Server 4.0 (IIS) with secure sockets layer (SSL) and you have installed a root certifying authority certificate (other than those issued by well-known third parties, such as Verisign, Thawte Consulting, or Microsoft), you may need to reinstall the affected root certifying authority certificates after you install SP4. You need to do this if you're using Microsoft Certificate Server 1.0, which shipped with the Windows NT Option Pack.

>>>To reinstall the root certifying authority certificate

1. Open Internet Explorer 4.0.
2. Browse to the root certifying authority certificate that you want to add. For example, for Microsoft Certificate Server, go to <http://server/certsrv/CertEnroll/cacerts.htm> and click the root certifying authority certificate you want.
3. Select Open this file from its current location, and then click OK.
4. Click Install certificate.
5. After the Certificate Manager Import wizard has started, click Next.
6. Select Place all certificates into the following store.
7. Click Browse, and then click Show physical stores.
8. Expand Trusted Root Certification Authorities, select Local Computer, and then click OK.
9. Click Next, and then click Finish.
10. Restart your Web server.

NOTE: There is no longer any need to use the IISCA.EXE tool.

-----

### 3.11 Message Queue Notes

-----

A new MSMQ registry entry helps you configure the MSMQ Service not to attempt to contact the MQIS at startup (to avoid auto-dialing, for

example). To activate that mode, under the "HKEY\_LOCAL\_MACHINE\Software\Microsoft\MSMQ\Parameters" registry key, add a value "DeferredInit", of type DWORD and with a value of 0x1. Add this only if the initial MQIS access causes unwanted dial-up, because this setting can delay applications calling MQOpenQueue in offline situations.

-----  
3.12 Installing COM Internet Services  
-----

3.12.1 Installing COM Internet Services

COM Internet Services (CIS) provides facilities for making DCOM calls over the Internet when other transports can't be used due to a firewall on the server side or a proxy server on the client's network. There are three configuration options for CIS:

1. Windows 95 or Windows 98 CIS Client Support
2. Windows NT 4.0 SP4 and Windows NT 5.0 CIS Client Support
3. Windows NT 4.0 SP4 and Windows NT 5.0 CIS Server Support

This topic explains how to install CIS on computers running Windows NT 4.0 SP4. If possible, you should start with client and server machines that aren't separated by either proxy servers or firewalls. Once you have verified that this configuration works correctly, you can add proxy servers or firewalls to the configuration.

3.12.2 Windows NT 4.0 SP4 CIS Client Support

For Windows NT 4.0, CIS requires that SP4 be installed on your Windows NT Workstation 4.0 or Windows NT Server 4.0 computer. To enable CIS, you need to add the Tunneling TCP protocol to the DCOM protocol list.

You can modify the protocol list by running DCOMCNFG:

1. Select the Default Protocols tab.
2. Use the Add button to add Tunneling TCP/IP.
3. Reboot the system to have this change take effect.

If multiple protocols are configured, DCOM attempts to use them in the order in which they appear in the DCOM protocol list.

3.12.3 Windows NT 4.0 SP4 CIS Server Support

For Windows NT 4.0, CIS requires that SP4 be installed on your Windows NT Server 4.0 computer. CIS also requires that Internet Information Server 4.0 (including the Internet Service Manager) be running. IIS 4.0 is part of the Windows NT 4.0 Option Pack.

1. Create an RPC subdirectory under your Inetpub directory. For example, at the command prompt, type

```
md c:\inetpub\rpc
```

This directory will be referred to as %inetpub%\rpc in the following instructions.

2. Copy Rpcproxy.dll from the Windows system directory to %inetpub%\rpc. For example, at the command prompt, type

# UNCLASSIFIED

copy %windir%\system32\rpcproxy.dll c:\inetpub\rpc

3. Create a virtual root for the directory you created. To do this:
  - \* Click Start, point to Programs, point to Windows NT 4.0 Option Pack, then Microsoft Internet Information Server, and then click Internet Server Manager.
  - \* In the left pane of the MMC window, select Console Root/IIS/<machine name>/Default Web Site.
  - \* Right-click Default Web Site, click Create New, and then click Virtual Directory.
  - \* In the New Virtual Directory wizard, enter the following:
    - alias to be used to access virtual directory = rpc
    - physical path = %inetpub%\rpc
    - permissions = Execute Access
4. Don't close Internet Service Manager. Change the connection timeout for the Default Web Site to 5 minutes. To do this:
  - \* In the left pane of the MMC window, select Console Root/IIS/<machine name>/Default Web Site.
  - \* Right-click Default Web Site, and then click Properties.
  - \* In the Default Web Site Properties dialog box, select the Web Site tab.
  - \* Change the Connection Timeout to 300.
  - \* Click OK. Do not close Internet Service Manager.
  - \* Install the RPC Proxy ISAPI Filter. To do this, run the IIS 4.0 Internet Service Manager, select Console Root/IIS/<machine name> in MMC, right-click the machine name, click Properties, select Edit for the Master WWW Service Properties, select the ISAPI Filters tab, select Add, and then type:
    - filter name = Rpcproxy
    - executable = %inetpub%\rpc\rpcproxy.dll
5. You can close Internet Service Manager now.
6. Enable CIS on the server. You do this by running DCOMCNFG. To do this:
  - \* Click Start, and then click Run.
  - \* In the Run dialog box, type dcomcnfg, and then click OK.
  - \* In the left pane of the MMC window, select the Default Properties tab.
  - \* Make sure the check box labeled Enable COM Internet Services on this computer is checked. Don't close DCOMCNFG.
7. Add the Tunneling TCP protocol to the protocol list. You can modify the protocol list by running DCOMCNFG. To do this:
  - \* Click Start, and then click Run.
  - \* In the Run dialog box, type dcomcnfg, and then click OK.
  - \* In the left pane of the MMC window, select the Default Protocols tab.
  - \* Use the Add button to add Tunneling TCP/IP.
  - \* Close DCOMCNFG.
8. Restart your computer to have these changes take effect.

## 3.12.4 Notes on Proxy Servers

If your client is located behind a proxy server, you need to ensure that:

- \* The proxy server is configured to enable the HTTP CONNECT verb for port 80.
- \* Your client computer is correctly configured to use the proxy server

to access the World Wide Web. To configure your client to use the proxy server, use the Internet control panel.

### 3.12.5 Notes on Firewalls

CIS requires that the firewall let through TCP/IP traffic on port 80.

-----  
3.13 Event Log Service  
-----

This Service Pack contains new features in the Event Log Service to assist how administrators measure the reliability and availability of Windows NT.

The SP4 Event Log Service records three new events in the system event log that are useful in measuring operating system availability.

\* Clean Shutdown Event (Event ID: 6006)

The Event Log Service records a clean shutdown event whenever an operating system shutdown is initiated. A clean shutdown can be initiated through several mechanisms: direct user interaction using the Shut Down screen; Shutdown/Restart using Ctrl+Alt+Delete; Shutdown/Restart using the Start Menu; Shutdown/Restart using the Logon screen. Clean shutdowns are also recorded if one of the following shutdown events happens programmatically: `InitiateSystemShutdown` WIN32 API (local), or `InitiateSystemShutdown` WIN32 API (remote).

\* Dirty Shutdown Event (Event ID: 6008)

The Event Log Service records a dirty shutdown event whenever the operating system is shut down via a mechanism other than a clean shutdown. The most common cause is when the system is power-cycled, i.e., Windows NT is stopped by powering off the system. The event is recorded upon the subsequent system reboot. While Windows NT Server is running, the system periodically writes a time stamp to the registry, which always overwrites the "last alive" time stamp from the previous interval. When the "last alive" time stamp is written, it's also flushed to disk. A normal clean shutdown is also flagged in the registry. If the clean shutdown flag isn't found on disk when an SP4 system reboots, a dirty shutdown event is recorded. The description part of the event contains the "last alive" time stamp. The "last alive" time stamp is written to the registry at a default interval of 5 minutes to `HKLM\Software\Microsoft\Windows\CurrentVersion\Reliability>LastAliveStamp`. Adding the registry DWORD value `TimeStampInterval` can change the interval. This value is in units of minutes. Setting it to zero prevents any "last alive" time stamp logging, only the boot and normal shutdown stamps will be written in that case.

\* System Version Event (Event ID: 6009)

The Event Log Service records a system version event containing the operating system version information whenever the system is booted. This makes it easier to post-process Windows NT system event logs by operating system version.

NOTE: Prior to SP4, the recording of operating system crashes in the event log (Save Dump events) was optional. By default, crash events were recorded but a system administrator could disable this behavior in the

System control panel by clearing "Write an event to the system log when a STOP error occurs" on the Startup/Shutdown tab. In SP4, the recording of crashes in the event log is mandatory for Windows NT Server and can't be disabled by an administrator. There is no change for Windows NT Workstation; an administrator can still choose either setting.

-----  
3.14 Upgrading a Cluster to SP4  
-----

3.14.1 Rolling Upgrade

You can eliminate the downtime of your cluster services and minimize administrative complexity by performing a rolling upgrade of the operating system. In a rolling upgrade, you sequentially upgrade the operating system on each node, making sure that one node is always available to handle client requests.

A rolling upgrade consists of four phases:

- \* Phase 1: Preliminary  
Each node runs Windows NT 4.0 Service Pack 3.
- \* Phase 2: Upgrade Node 1  
Node 1 is paused, and Node 2 handles all cluster resource groups while you upgrade the operating system of Node 1 to Windows NT 4.0 Service Pack 4.
- \* Phase 3: Upgrade Node 2  
Node 1 rejoins the cluster. Node 2 is paused and Node 1 handles all cluster resource groups while you upgrade the operating system on Node 2 to Service Pack 4.
- \* Phase 4: Final  
Node 2 rejoins the cluster.

The operation of Phase 3, when the two cluster nodes run different service packs, is called a "mixed-version cluster." It's recommended that you ensure that every resource on your cluster can operate in a mixed-version environment. If version incompatibilities prevent a cluster resource from operating in a mixed-version cluster, you won't be able to successfully complete your rolling upgrade.

NOTE: You can't create new groups, resources, or resource types in a mixed-version cluster.

>>>To perform a rolling upgrade

1. Pause the cluster service on Node 1 and move its resource groups to Node 2.
2. Upgrade Node 1 from Service Pack 3 to Service Pack 4.
3. Perform validation tests on Node 1 to certify that the node is fully functional.
4. In Cluster Administrator, click Resume Node.
5. Repeat steps 1 through 4 for Node 2 instead of Node 1.

### 3.14.2 Alternatives to a Rolling Upgrade

There are two alternatives to a rolling upgrade for upgrading Windows NT on a cluster.

If you can't perform a rolling upgrade because your cluster manages a resource that is incompatible with rolling upgrades, you should consider taking the incompatible resource offline, performing a rolling upgrade, then installing the new version of the resource.

If most of your cluster resources are incompatible with a rolling upgrade, you should consider a clean install of Microsoft Cluster Server. If you do this, you must reconfigure your cluster after the installation.

>>>To perform a clean install of Microsoft Cluster Server

1. Following the procedure described in Cluster Administrator Help, stop the cluster service on Node 1. On Node 1, uninstall Microsoft Cluster Server.
2. Stop the Cluster Service on Node 2. On Node 2, uninstall Cluster Server. At this point, the cluster that had been running on Node 1 and Node 2 no longer exists.
3. Reinstall Cluster Server on Node 1 using the Windows NT 4.0 Enterprise Edition Components CD, and then form a new cluster using the name of the original cluster.
4. Reinstall SP4 and perform validation tests on Node 1. SP4 upgrades the original SP3 clustering product to SP4.
5. Reinstall the Cluster Server on Node 2 using the Windows NT 4.0 Enterprise Edition Components CD, and then join the newly formed cluster.
6. Reinstall Cluster Server, and then perform validation tests on Node 2.
7. Using Cluster Administrator, add cluster resources to your new cluster.

### 3.14.3 Known Clustering Issues

You won't be able to select or clear the Use network name for the computer name check box on the Generic Service Parameters tab if you change the value for the resource from its original setting. The service uses the network name for the computer name, regardless of the check box value. To fix the problem, open Regedt32 and edit the following key on all the cluster nodes:

HKLM\SYSTEM\CurrentControlSet\Services\\Environment

This is a multiline string. Remove the line containing `_CLUSTER_NETWORK_NAME_`.

=====  
4.0 ADDITIONAL FIXES AND WORKAROUNDS  
=====

This section contains additional fixes and workarounds for this Service Pack release.

-----  
4.1 Installing Windows NT 4.0 on a Windows NT 5.0 Computer  
-----

When installing Windows NT 4.0 on a computer that has Windows NT 5.0 Beta or later installed, Setup may continuously reboot at the boot menu after the initial text mode phase of Windows NT 4.0 Setup.

The updated Winnt32.exe in the Support\Winnt32 folder allows you to install Windows NT 4.0 on a computer already running Windows NT 5.0.

>>>To update the Winnt32.exe

1. Obtain the Winnt32.exe file from Windows NT 4.0 Service Pack 4, and copy the file to a folder on your hard disk, or double-click the file on the Service Pack 4 CD-ROM. The Winnt32.exe file is located in the Support\Winnt32 folder.
2. When you are prompted for the location of the Windows NT 4.0 files, supply the path to the \i386 folder or \Alpha on the Windows NT 4.0 CD-ROM.

For more information, go to the Microsoft Knowledge Base at <http://support.microsoft.com/> and search for KB article Q185322.

>>>After Windows NT 4.0 is installed

1. Apply Service Pack 4.
2. Copy NTLDR and NTDETECT.COM from the Windows NT 5.0 CD to the root of the system drive.

NOTE: To use this installation method, the partition you install to must contain the FAT file system.

-----  
4.2 Dual Booting Between Versions of Windows NT 4.0 and Windows NT 5.0  
-----

When installing a dual-boot system on your computer to access both Windows NT 4.0 and Windows NT 5.0, each installation or instance of Windows NT must have a unique computer name.

NOTE: This is required only if your dual-boot computer is on the same Windows NT domain.

-----  
4.3 NTFS Version 4 and NTFS Version 5 Support  
-----

There are two recent versions of Windows NT File System (NTFS):  
\* version 4--supported by both Windows NT 3.51 and Windows NT 4.0  
\* version 5--supported by Windows NT 5.0  
This Service Pack contains an updated version of NTFS.sys that can also read NTFS 5 volumes.

NOTE: The following scenarios don't support dual-boot systems:

- \* Pre-Windows NT 4.0 Service Pack 3 installations.
- \* Windows NT 3.51 or earlier installations.

These features of NTFS version 5 can't be accessed from SP4, even

with the updated NTFS.sys:

- \* Release points (also called mount points or junction points)
- \* Native Structured Storage (NSS) files
- \* Encrypting File System (EFS)
- \* Disk Quotas

Attempts by Windows NT 4.0 Service Pack 4 users or applications to access release points or NSS files created on NTFS version 5 drives with a Windows NT 5.0 installation will fail, usually with an "access denied" error.

Antivirus applications may report to the user (log file, popup dialog, or both) when a file can't be accessed. These applications may report failure to access NSS files with extensions the applications are set to scan. Archiving programs cannot add NSS files to an archive, and this might be reported as an error. Backup programs won't back up NSS files or release points as expected. They may log the failures as either "file in use" or "file not available." Some backup applications fail when trying to verify folders that contain NSS files during the backup process.

When mounting an NTFS 5.0 volume under Windows NT 4.0 SP4, NTFS 5.0 features are unavailable and chkdsk can't be performed against the volume. However, most read/write operations function normally if they don't make use of any NTFS 5.0 features. Also, since files can be read and written on NTFS 5.0 volumes under Windows NT 4.0, Windows NT 5.0 may need to perform "clean-up" operations by running chkdsk on the volume after it was mounted on Windows NT 4.0. These clean-up operations ensure that the NTFS 5.0 data structures are consistent after an Windows NT 4.0 mount operation.

-----  
4.4 Installing SP4 on a Windows NT Server Enterprise Edition System  
-----

If you upgrade from Windows NT Server 4.0 with SP4 to Windows NT Server Enterprise Edition using the Winntup.exe upgrade, a popup occurs at every reboot that prompts you to install Service Pack 3. If you try to install SP3, you're notified that a newer service pack is installed. To work around this, install SP4 again, which will resolve the problem. The popup won't appear if you install SP4 over Windows NT Server Enterprise Edition, or if you upgrade from Windows NT Server using Winnt32.exe.

-----  
4.5 Internet Information Server 4.0  
-----

4.5.1 Username/Password Length

The length limitation for Username/Password combinations when using Internet Information Server 4.0 has been fixed in SP4. This previously caused errors when using basic authentication on IIS 4.0.

4.5.2 Global.asa

To use the Global.asa file after applying SP4, ensure that the file is in an application root folder. This is a change from the implementation in the Windows NT Option Pack, in which Global.asa was mistakenly processed from within a virtual directory.

The Global.asa file specifies event scripts and declares objects that have session or application scope. In the Windows NT Option Pack, the file Asp.dll processed Global.asa from the lowest defined virtual directory. This has been changed in SP4. After SP4 is installed, customers who are using Global.asa may need to make changes to IIS for the file to work properly. For more information, see the "Global.asa Reference" topic in the Windows NT Option Pack online documentation.

To ensure that Global.asa is available to Asp.dll after applying SP4, folders that contain Global.asa files should be marked as applications. For more information, see the "Creating Applications" topic in the Windows NT Option Pack online documentation.

Certain CryptoAPI-related file name extensions (.cer, .crt, and .der) aren't registered correctly when Internet Explorer 4.0 is installed after SP4. To restore the file name extension registration, run the following command line:

```
Regsvr32.exe cryptext.dll
```

-----  
4.6 Security Configuration Manager  
-----

4.6.1 Error Messages Received When Logging on to a Secure Desktop  
The first time a user logs on to a Compatible, Secure or Hi Secure Windows NT system running Internet Explorer 4.0 or later, the following error message appears:

INF Install Failure. Reason: Access is denied.

Corresponding Start Menu Items are missing.

To work around this error message, have potential users of the system log on prior to securing the desktop.

4.6.2 Incorrect Analysis When Registry Key Doesn't Exist  
If a registry value doesn't exist, analysis results for that registry value may be inaccurate. To work around this, configure the registry value to the appropriate setting. This problem will be fixed in the next release of Windows NT.

4.6.3 Inherit Mode Not Available  
Administrators can decide how SCM configures child objects after Access Control Settings for file system and registry objects are defined. The options are: Inherit, Overwrite, or Ignore. In Windows NT 4.0, the Inherit option is grayed out and therefore, not available.

-----  
4.7 Updating Audio Drivers  
-----

If you aren't receiving audio from a Crystal Semiconductor audio chip or a Creative Labs Sound Blaster AWE32 Plug and Play Wavetable Synthesizer, you may need to install the updated drivers for these devices. For detailed information on updating these drivers, go to

the Microsoft Knowledge Base at <http://support.microsoft.com/> and search for KB article Q143155.

-----  
4.8 Microsoft Proxy Server  
-----

4.8.1 Web Administration Tool

After the SP4 is installed, the Web Administration Tool for Microsoft Proxy Server 2.0 may stop working. This is because Internet Information Server doesn't have the correct application setting for the Proxy Server Web administration tool, which requires script execute permission. This problem may only occur with Windows NT Server 4.0, Service Pack 4, and Windows NT 4.0 Option Pack. To correct the problem, follow the steps below:

1. Click Start, point to Programs, point to Windows NT 4.0 Option Pack, point to Microsoft Internet Server, and then point to Internet Service Manager.
2. Click Internet Information Server in the left pane.
3. Double-click your server name in the right pane.
4. Double-click MS Proxy Administration Web Site in the right pane.
5. In the right pane, right click PrxAdmin, and then click Properties.
6. Click the Virtual Directory tab.
7. In the Application Settings section, set the Permissions to "Script."
8. In the Application Settings section, click Create. If a Remove button is displayed and there isn't a Create button, no further action is necessary (the system is already properly configured).
9. Click OK.

You may have to reboot your computer.

4.8.2 Microsoft Proxy Server 1.0 Client

Installing SP4 on a Windows NT 4.0 Workstation or Server with Microsoft Proxy Server 1.0 client installed causes the WinSock Proxy Client component to be disabled. As a result, applications that access the Internet and depend on the Proxy client may not be able to access the Internet. To correct the problem, reinstall the Proxy Server Client component after you install SP4. It's recommended that you uninstall the Microsoft Proxy Client before installing SP4. After SP4 is installed, the Proxy Client can be reinstalled.

=====  
5.0 APPLICATION NOTES  
=====

This section includes application notes for this Service Pack release.

-----  
5.1 CheckIt Diagnostic Kit 4.0 by Touchstone  
-----

The CheckIt Diagnostic Kit version 4.0 won't have full functionality when installed on top of any version of Windows NT.

-----  
5.2 Norton CrashGuard 2.0 for Windows NT  
-----

Norton CrashGuard 2.0 for Windows NT requires that a user who has administrative privileges install the product for the service to start

when a computer is rebooted.

-----  
5.3 Inoculan 4.0  
-----

The Inoculan version 4.0 Service Pack 2, with build number 373 or higher, is fully compatible with SP4. The previous release of Inoculan 4.0 Service Pack 1 with build 270 will cause Windows NT 4.0 bugcheck when you apply the SP4.

You can download the Inoculan SP2A build 375 (il0145i.zip) from <http://www.cai.com>.

-----  
5.4 Exceed  
-----

If you use Exceed Inetd.exe to provide basic telnet services in Windows NT 4.0, contact Hummingbird Software at <http://www.hummingbird.com> for an update. The version that ships with Exceed 6.0.1 doesn't work with SP4.

-----  
5.5 Terminal Server  
-----

SP4 isn't supported on Windows NT Terminal Server. There will be a revision of SP4 made specifically for Terminal Server that will include the information required to allow existing installed applications to run in a multisession environment. Obtain this revision to install SP4 on a Windows NT Terminal Server.

-----  
5.6 Microsoft NetMeeting Security and Y2K Issues  
-----

5.6.1 Security

NetMeeting 2.1 is vulnerable to maliciously-created speed-dial objects that can cause NetMeeting to crash. After NetMeeting has crashed, the computer's memory is exposed and may be intentionally corrupted. To work around this, download the Speed Dial patch from <http://www.microsoft.com/netmeeting>.

5.6.2 Y2K

When transferring a file with a system date greater than 2000, the received file date is increased by 28 years. To work around this, download NetMeeting version 2.1 (or later) at <http://www.microsoft.com/netmeeting>.

-----  
5.7 Numega SoftICE  
-----

If you try installing SP4 and you aren't using the latest version of SoftICE, version 3.24, a message appears stating that Windows has detected a version of SoftICE that isn't supported.

You can register and download the latest version of SoftICE from <http://www.numega.com/support/updates.htm>. Earlier revisions of the SoftICE software cause system errors when installing SP4. SoftICE

# UNCLASSIFIED

version 3.24 is a no-charge update for registered version 3.2 customers.

If your version of SoftICE is prior to 3.2, contact the Numega sales department at 1-800-4NUMEGA (or 1-603-578-8400) to purchase an upgrade.

-----  
5.8 Microsoft BackOffice Small Business Server  
-----

5.8.1 Windows NT 4.0 Year 2000 Issues

(a) You must be running Microsoft BackOffice Small Business Server (SBS) version 4.0a.

If you have SBS 4.0, then installing SBS 4.0 Service Pack 1 updates your server to SBS 4.0a.

>>>To check the version number

1. Click Start, and then point to Manage Server.
2. Click "About Microsoft Small Business Server" in the upper right hand corner.
3. The version will be displayed if you have version 4.0a or greater.
4. If a version number isn't displayed, then you have version 4.0.

See <http://www.microsoft.com/backofficesmallbiz> for instructions on how to order SBS 4.0 Service Pack 1 or call 1-800-370-8758.

(b) Install Windows NT 4.0 Service Pack 4 by running Update.exe  
After you install SP4 and the server reboots, you may be prompted to install additional components to resolve known Year 2000 issues for Windows NT 4.0.

(c) For more information on known SBS 4.0 Year 2000 issues, consult <http://www.microsoft.com/backofficesmallbiz>

5.8.2 Microsoft BackOffice Small Business Server version 4.0

\* Upgrade to SBS 4.0a prior to installing Windows NT 4.0 SP4. You can do this by installing SBS 4.0 Service Pack 1. See <http://www.microsoft.com/backofficesmallbiz> for instructions on how to order SBS 4.0 Service Pack 1 or call 1-800-370-8758.

\* You must install SBS 4.0 Service Pack 1 before installing Internet Explorer 4.0 or 4.01.  
IMPORTANT: Don't install IE 4.0 or IE 4.01 on SBS 4.0. This results in the loss of functionality to the "Manage Server" administration console.

\* If you install SBS 4.0 SP1 after installing Windows NT 4.0 SP4, you will see a series of dialog boxes asking if you would like to replace newer files with older files. Click "No to All" so that the newer SP4 files remain on your computer.

5.8.3 Microsoft BackOffice Small Business Server version 4.0a

Install Windows NT 4.0 Service Pack 4 by running Update.exe. After Windows NT 4.0 Service Pack 4 installation is complete, and the server reboots, you may be prompted to install additional components to resolve known Year 2000 issues in Windows NT 4.0.

5.8.4 Microsoft Proxy 1.0 on Small Business Server 4.0 and 4.0a  
Installing Windows NT 4.0 Service Pack 4 on an Small Business Server

4.0 (SBS) server disables the Winsock Proxy Client component. As a result, some applications that access the Internet and depend on the proxy Dial-On-Demand won't work on the SBS server. To correct the problem, reinstall the Proxy Client component after you install Windows NT 4.0 SP4. To reinstall the Proxy Client, click Start, point to Programs, point to Startup, point to Microsoft Proxy Client, and then click Setup.

5.8.5 Windows NT Workstation 4.0 Client for Microsoft BackOffice Small Business Server 4.0 and 4.0a

If you run Windows NT 4.0 Service Pack 4 Update.exe on an SBS 4.0 or 4.0a Windows NT 4.0 Workstation client, you may be prompted with a dialog box stating that SBS 4.0 has been detected on your computer. Please refer to Section 2.4, "Year 2000 Service Pack Installation" for instructions of this document and <http://www.microsoft.com/backofficesmallbiz> for more information on known Year 2000 Windows NT issues.

-----  
5.9 Rational Visual Quantify Version 4  
-----

If you install SP4 on a system with Rational Visual Quantify version 4 installed, you may get .dll error messages. To work around this, reinstall Rational Visual Quantify after you install SP4.

-----  
5.10 Microsoft IntelliPoint  
-----

If you receive an access violation from IntelliPoint Productivity Tips, Tips.exe, when starting Windows NT 4.0 SP4, we recommend that you install the latest version of IntelliPoint software, available from the Microsoft Web site at <http://www.microsoft.com/products/hardware/mouse/>.

=====  
6.0 LIST OF BUGS FIXED IN WINDOWS NT 4.0 SERVICE PACKS 1-4  
=====

All bug fixes contained in Service Packs 1-4 are documented as Knowledge Base articles. You can query the Knowledge Base to find an article about a specific bug by using the Qxxxxxx number that is assigned to the bug. You can browse the Knowledge Base on the Microsoft Web site at <http://support.microsoft.com/support/>.

For a list of all bug fixes in Windows NT 4.0 Service Packs 1-4, see <http://support.microsoft.com/support/kb/articles/q150/7/34.asp>.

=====  
7.0 DEPLOYMENT NOTE FOR SERVICE PACK 4 (128-BIT VERSION)  
=====

System administrators and others who anticipate corporate-wide deployment of this product should consult [Faq.txt](#) for specific cautions regarding the nature of this high-encryption product.

If you plan to install this product on a computer and travel out of the country with that computer, consult [Faq.txt](#) for cautions and requirements regarding the nature of this high-encryption product.

=====

8.0 EXPORT RESTRICTIONS FOR SERVICE PACK 4 (128-BIT VERSION)

=====

The North American (128-bit) version of Service Pack 4 is intended for distribution only in the United States and Canada. Effective January 1, 1997, export of this Service Pack from the United States is regulated under "EI controls" of the Export Administration Regulations (EAR, 15 CFR 730-744) of the U.S. Commerce Department, Bureau of Export Administration (BXA). EI controls are the current equivalent of ITAR munitions export controls that previously applied to this product. EI controls require that you obtain a Commerce export license prior to any export, transmission, or shipment of this product to any country, other than Canada, or to any person, entity, or end user subject to U.S. export restrictions. For further information, the Commerce export license process and EI controls are described on the BXA Web site at <http://www.bxa.doc.gov/encstart.htm>.

Microsoft will distribute the North American (128-bit) version of Service Pack 4 to U.S. or Canadian companies or persons for end-use in the U.S. or Canada only.

=====

9.0 STRONG ENCRYPTION SUPPORT IN THIS SERVICE PACK 4 (128-BIT VERSION)

=====

Available through Windows NT 4.0 Service Pack 4, CryptoAPI provides developers with access to standards-based, core cryptographic functionality. An Enhanced Cryptographic Service Provider is included in this Service Pack, allowing applications that call CryptoAPI to use stronger keys and new algorithms. Algorithm support has been extended to include DES and Triple DES. Keylengths have been extended for RC2 and RC4 ciphers to 128-bits; RSA Keylengths have been lengthened to allow up to 16K-bit keys.

This Service Pack also includes 128-bit support for Remote Access Server (RAS). Wide area connections made using RAS on both Windows NT Workstation and Windows NT Server will use a 128-bit key to encrypt data, thus providing a more secure connection.

Secure Sockets Layer (SSL) is used today by Internet browsers and servers (including Microsoft Internet Explorer and Microsoft Internet Information Server) for message integrity and confidentiality of communications and for optionally mutual authentication. With SSL, parties using the Internet can be confident that their communications are private and haven't been tampered with or altered. The version of SSL shipped with this Service Pack uses 128-bit encryption.

Secure Remote Procedure Call (RPC) has also been enhanced to support 128-bit encryption. Any application that requests secure RPC will automatically use 128-bit encryption.

Installing SP 4 (128-bit version) will update your system with all of the strong encryption support.

## (U) List of Bugs Fixed in Windows NT 4.0 Service Packs

(U) This is the complete formatted text from Microsoft Knowledge Base Article Q150734 available from Microsoft at <http://www.microsoft.com>.

List of Bugs Fixed in Windows NT 4.0 Service Packs

Last reviewed: October 21, 1998

Article ID: Q150734

The information in this article applies to:

- \* Microsoft Windows Workstation version 4.0 Service Pack 4
- \* Microsoft Windows Server version 4.0 Service Pack 4
- \* Microsoft Windows Workstation version 4.0 Service Pack 3
- \* Microsoft Windows Server version 4.0 Service Pack 3
- \* Microsoft Windows Workstation version 4.0 Service Pack 2
- \* Microsoft Windows Server version 4.0 Service Pack 2
- \* Microsoft Windows Workstation version 4.0 Service Pack 1
- \* Microsoft Windows Server version 4.0 Service Pack 1

### SUMMARY

This article is a current listing of the article numbers for bugs that were fixed in the latest Windows NT 4.0 Service Pack. Use the Qxxxxxx number that precedes the title of the bug fix to query the Microsoft Knowledge Base to find an article about that bug.

NOTE: If an article appears in the Readme.txt file for the service pack, but does not appear in the following list, it is because the article was mistakenly added to the Readme.txt file.

### MORE INFORMATION

#### Service Pack 4

- \* Q109993 Winsock Application Causes 0x0000000A Blue Screen STOP Message
- \* Q112547 Dial-Up Networking Hangs After Failed Multilink Attempt
- \* Q123597 WinNT Err Msg: Error 614 Out of Buffers When Using RAS Script
- \* Q125020 NetBIOS SEND WAIT Call Returns Before RECEIVE is Sent
- \* Q129047 Synchronizing DNS Information in Registry with Boot Files
- \* Q129457 Anonymous Connections May Be Able to Obtain the Password Policy
- \* Q137565 System Error 53 When Connecting to a FQDN
- \* Q138791 SCSI Printing Devices Requiring Wide SCSI May Fail
- \* Q141496 DHCP Client Comment Disappears When Obtaining IP Address
- \* Q141708 Printing to LPD Printer Is Slow or Fails with Windows NT
- \* Q142026 Err: "Hidden Console of WOW VDM" Running 16-bit or MS-DOS App
- \* Q142047 Bad Network Packet May Cause Access Violation (AV) on DNS Server
- \* Q142615 Event Log Service Fails to Check Access to Security Log File
- \* Q142635 Cannot Change the Drive Letter of Removable Drives
- \* Q143160 Enterprise Server Stops During Print Spooling
- \* Q143478 Stop 0A in Tcpi.sys When Receiving Out Of Band (OOB) Data
- \* Q143484 IIS Services Stop with Large Client Requests
- \* Q146095 STOP: 0x0000000A or STOP: 0x0000001E in Tcpi.sys

## UNCLASSIFIED

- \* Q146965 GetAdmin Utility Grants Users Administrative Rights
- \* Q147222 Group of Hotfixes for Exchange 5.5 and IIS 4.0
- \* Q147706 How to Disable LM Authentication on Windows NT
- \* Q149658 TCP/IP Printing Causes File Cache to Grow
- \* Q150953 Nwuser.exe Send Function Truncates Messages to 38 Characters
- \* Q151677 NWLink SPX Ignores Allocation Number Sent By Peer
- \* Q151778 Huge Downlevel Print Job Causes File Cache to Grow
- \* Q151860 STOP 0x0A While Writing to the Middle of a Cached File
- \* Q152079 SNMP Traps Contain Invalid Agent ID Field
- \* Q152764 Garbled Characters Appear in Windows NT Print Queue
- \* Q152993 Raster Fonts Print Different on Windows NT 4.0 Than on 3.51
- \* Q153161 WinNT Systems Running RAS May Exhaust Available DHCP Leases
- \* Q153296 Write Cache on IDE/ATAPI Disks Is Not Flushed on Shut Down
- \* Q154087 Access Violation in LSASS.EXE Due to Incorrect Buffer Size
- \* Q154094 Using Iomega ATAPI Zip Drives with Windows NT
- \* Q154162 Memory Leak in Perfmon.exe Occurs Monitoring WINS Counters
- \* Q154174 Invalid ICMP Datagram Fragments Hang Windows NT, Windows 95
- \* Q154387 TAPISRV.EXE Thread Uses Excessive CPU Time
- \* Q154398 BDC Secure Channel May Fail if More Than 250 Computer Accounts
- \* Q154460 Denial of Service Attack Against WinNT Simple TCP/IP Services
- \* Q154475 Add Printer Wizard Printer Browse List Not in Alphabetical Order
- \* Q154552 NETSTAT Causes Memory Leak
- \* Q154694 New Policy Available to Hide Go To on Tools Menu
- \* Q154791 MS-DOS-based Applications May Not Find All Files
- \* Q154984 DNS Server May Not Recursively Resolve Some Names
- \* Q154985 DNS Registry Key Not Updated When Changing Zone Type
- \* Q154990 SETPASS May Change Password of Wrong User
- \* Q155495 Reference Counter Overflow in Security Descriptor Causes STOP
- \* Q155701 Invalid UDP Frames May Cause WINS to Terminate
- \* Q156655 Memory Leak and STOP Screens Using Intermediate NDIS Drivers
- \* Q157032 Services for Macintosh May Cause STOP 0x0A During High Load
- \* Q157123 Communicating with SNA Hosts May Cause STOP 0x0A in DLC.SYS
- \* Q157182 FPNW Causes STOP 0x50 When Connection Is Closed Twice
- \* Q157911 Deadlock in Service Control Manager During System Shut Down
- \* Q157913 Services Set to Interact With Desktop May Fail to Start
- \* Q158396 Explorer Hangs When Creating a New Folder On a MAC Volume
- \* Q158516 Access Violation in RPCRT4.DLL When Pickling Buffered RPC Data
- \* Q158548 Sysdiff Changes Dates on Files It Applies to Windows NT
- \* Q158581 Icon Position Not Stored When Using Roaming Profiles
- \* Q158682 Shortcuts Created Under Windows NT 4.0 Resolve to UNC Paths
- \* Q158706 Netmon Performance Counters Support a Maximum of Eight Adapters
- \* Q159310 Updated Version of Dns.exe Fixes Several Problems
- \* Q159595 Missing Uppercase "A" Character in the 1257 Font
- \* Q159599 WINS Consistency Checking May Not Start at Scheduled Time
- \* Q159839 Sysdiff Does Not Add Empty Directories
- \* Q159909 STOP 0x0000000A May Occur on Multiprocessor Systems
- \* Q160517 RRAS May Decrement Local Static Route Metric
- \* Q161968 NetBT Tears Down TCP Session with Many Concurrent File Transfers
- \* Q161969 LPR Printing Device Reports an Error If Printer Not Available
- \* Q162230 Fragmentation and Performance Issues with PPTP Connections
- \* Q163055 DHCP Client May Fail with WinNT 4.0 SP2 Multinetted DHCP Server
- \* Q163251 STOP 0xA Due to Buffer Overflow in NDISWAN.SYS
- \* Q163662 Running Multiple Instances of an Application Causes STOP x50

# UNCLASSIFIED

- \* Q163852 Invalid Operand with Locked CMPXCHG8B Instruction
- \* Q163855 STOP 0x0000001e May Occur in Srv.sys w/ Down Level Client
- \* Q164023 Fix for Gethostbyname() IP Address Order on Local Multihomed Mac
- \* Q164253 WinNT Err. Msg: Event ID 2018 When Srv.sys Is out of Memory
- \* Q164314 WinNT Err Msg: STOP 0x0000001E in Win32k.sys When Moving Mouse
- \* Q164438 FPNW Print Jobs Do Not Print or Errors Occur in FPNW Interface
- \* Q165005 Windows NT Slows Down Because of Land Attack
- \* Q165181 EISA Configuration Boot Code Is Replaced on Mirror Drives
- \* Q165387 Sharing Violation When Deleting a Folder
- \* Q165404 NTVDM AV on Servers with Exchange cc:Mail Connector
- \* Q165439 Parsing LMHOSTS with Invalid Entries Can Cause Stop 0x1E
- \* Q165664 RPC Encoding API "MesInqProcEncodingId" May Not Work
- \* Q165989 GetPeerName() Returns WSAENOTCONN After Select() Returns Success
- \* Q166571 Creating an SFM Volume on Large Partition Causes a Stop 0x24
- \* Q166822 Remote Password Change Works Incorrectly to Down-Level Server
- \* Q166846 Cannot Reconnect to TN3270 Server with Close Listen Sockets
- \* Q167038 RAS Clients Run Winsock and RPC Applications Slowly
- \* Q167040 PPTP Performance Update for Windows NT 4.0 Release Notes
- \* Q167110 WinNT Err. Msg: Stop 0x1E in FPNWSRV.SYS
- \* Q167395 RIP Routes May Expire Early When Running Windows NT 4.0 RIP
- \* Q167629 Predictable Query IDs Pose Security Risks for DNS Servers
- \* Q167703 Canon Bubble Jet BJC-4300 Does Not Support Ledger Paper
- \* Q167708 BootP Client Names Disappear in DHCP Manager
- \* Q167871 Error When Connecting to a Share on WinNT 4.0 NTFS Partition
- \* Q167969 Under Windows NT, Win16 Applications Opening MS-DOS Devices Fail
- \* Q168076 WINS Fails to Converge
- \* Q168662 DLC May Fail When Connecting Through an IBM 2210 Router
- \* Q168748 Java Applets Cause IE 3.02 to Stop Responding w/ SP3
- \* Q169020 32-bit Help Fails to Start When 16-bit Help Is Running
- \* Q169131 Print Setup Dialog Box May Take a Long Time to Display
- \* Q169274 TCP/IP Causes Time Wait States to Exceed Four Minutes
- \* Q169291 Using Scopes with Different Subnet Masks in a Superscope
- \* Q169404 NTFS Directory Corruption with Frequent File Creation
- \* Q169461 Access Violation in DNS.EXE Caused by Malicious Telnet Attack
- \* Q169608 Occasional File Corruption When Using Unbuffered I/O
- \* Q169822 DSMN RAS Dial-in Properties Deletes NetWare Compatibility
- \* Q169839 XFOR: Cannot Enable (Appletalk) MTA Service NT SP3
- \* Q169847 SNMP SysUpTime Counter Resets After 49.7 Days
- \* Q169888 User-Define Path Dropped When User and System Paths Too Large
- \* Q170057 Dr. Watson Dialog Box Stops Responding
- \* Q170509 Memory Leak in SERVICES.EXE Causes Performance Degradation
- \* Q170510 Double-Clicking the Mouse Button Acts as a Single Click
- \* Q170517 Cannot Log on Using IPX After Installing SP3 on Windows NT 4.0
- \* Q170518 DNS Admin Fails When Managing Large Number of Zones
- \* Q170534 Microsoft FTP Client Echoes Gateway Password on the Screen
- \* Q170566 Ntbackup.exe Log Has Additional Space at Beginning of Each Line
- \* Q170568 Seagate Tape Drive Light Stays Lit After Exiting NTBACKUP
- \* Q170572 Unable to Format a 1.44-MB Disk on an LS-120 After SP3
- \* Q170626 DDEML: Memory Leak in Global Shared Memory
- \* Q170753 Window Focus Set to Invoke Wrong 16-bit Application Through DDE
- \* Q170817 Windows NT Causes APC Smart UPS Battery to Discharge
- \* Q170880 Diskdump.sys Common Buffer Size Is Changed
- \* Q170965 SFM Time and Date Stamp Change Copying Between Volumes Locally

## UNCLASSIFIED

- \* Q171180 Non-Paged Pool Memory Leak in IRP Pool Tag
- \* Q171181 Deadlock in TCP/IP on Multiprocessor Computers
- \* Q171213 Copy to Removable Drive in Explorer May Fail After Media Swap
- \* Q171295 Fault Tolerant Systems May Encounter Problems with WinNT SP3
- \* Q171307 How to Disable SAP Broadcast for RPC Service
- \* Q171308 Explorer File Properties Dialog Version Tab Missing
- \* Q171386 Connectivity Delay with Multiple Redirectors Installed
- \* Q171458 Windows NT May Fail On Request to Open Large Files
- \* Q171564 TCP/IP Dead Gateway Detection Algorithm Updated for Windows NT
- \* Q171790 Time Incorrect After Restarting Multiprocessor System
- \* Q171940 MS-DOS Application I/O Operations Cause Floppy Drive Access
- \* Q171989 Windows NT Services for Macintosh May Not Start in Desired Zone
- \* Q171996 Winsock Function Calls Generate Non-Paged Pool Memory Leak
- \* Q171997 WINS Replication Does Not Start As Scheduled
- \* Q172003 Macintosh Change Password Fails on Down Trusted Domain PDC
- \* Q172030 WinNT Err Msg: Stop 0xA in TCPIP.SYS
- \* Q172122 Toshiba I586 Pro 230 MHz System and the National 307 Chip
- \* Q172147 Add Printer Wizard Hangs When Searching for Remote Printers
- \* Q172290 Routing and Remote Access "Out of Buffers" Event Logs
- \* Q172511 Stop 0x0000000A w/ Services for Macintosh & McAfee Anti-Virus
- \* Q172512 Routing and Remote Access Event ID 20100
- \* Q172613 Errors Connecting Through RAS When Password Expires
- \* Q172705 Explorer Access Violates When Viewing a File's Properties
- \* Q172762 Continuous Bhnt.sys Load and Unload Causes STOP 0xA and 0x7F
- \* Q172885 NetWare Print Server Names With Periods Truncated in Explorer
- \* Q172930 Removing Bypass Traverse Checking Causes Copy to Drop Streams
- \* Q172982 16-bit ShellExecute Fails if Application Exists in Long Path
- \* Q173059 Security Events Are Not Logged During Audit
- \* Q173277 No Memory.dmp File Created with RAM Above 1.7 GB
- \* Q173322 How to Disable Autochk During a Windows NT Reboot
- \* Q173385 System Policy Editor Will Not Allow More Than 255 Characters
- \* Q173523 IIS 3.0 Can Fail in Low Memory Conditions
- \* Q173525 WINS Client May Switch Primary and Secondary WINS Servers
- \* Q173526 "Serious Disk Error" When Saving Word 6.0 Document on Windows NT
- \* Q173533 WinNT Radius Client Sends Incomplete Accounting Information
- \* Q173676 Client Cannot Resolve MX Record via Microsoft DNS Server
- \* Q173753 Duplicate IP Addresses After Upgrading DHCP Clients to SP2
- \* Q173817 Savedump.exe Now Provides More Security to Memory.dmp
- \* Q173881 STOP 0x0000000A in Netbt.sys on a Multiprocessor Computer
- \* Q173941 Windows NT DNR Does Not Cache Short Names
- \* Q173993 Dialog Message Not Sent Correctly from 32-bit to 16-bit App
- \* Q173994 GetTextExtentPoint32W May Fail with Unicode Characters > 0x
- \* Q173997 Drive Letter Not Displayed in Error Message Box
- \* Q173998 Middle East/Thai Windows NT May Print Incorrect Characters
- \* Q174020 STOP 0x0000001E During Forced Shutdown and Program Exit
- \* Q174058 Delayed Worker Threads Causes a STOP 7A
- \* Q174076 Invalid Password Message When Strong Passwords Are Required
- \* Q174187 WinNT Does Not Display IBM PS/2 TrackPoint as the Mouse Driver
- \* Q174205 LSASS May Use a Large Amount of Memory on a Domain Controller
- \* Q174233 KelnitSystem Function Returns Uninitialized Stack on Alpha
- \* Q174234 Computer Hangs with Intensive 16-bit Code Running in a VDM
- \* Q174266 "Print Screen" from MS-DOS Application May Print Twice
- \* Q174333 Installing Win95 Print Drivers on WinNT 4.0 Asks for Wrong Disk

# UNCLASSIFIED

- \* Q174465 Bad SAP Packet Causes 0x0000000A In Afd.sys
- \* Q174478 Minimizing or Maximizing Does Not Redraw Window Properly
- \* Q174502 Fault Tolerant Recovery Does Not Reoccur After Shut Down
- \* Q174509 Stop 0x0000000A in Ndiswan.sys with Digiboard ISDN Board
- \* Q174510 Print Job Corruption Printing on Fast Hardware Across Slow Link
- \* Q174531 DirectDraw Fails Surface Creation with Large Dimensions
- \* Q174534 BitBit May Not Work When Raster Operation Mode Is NOTSRCCOPY
- \* Q174535 Access Violation When TCMAPP Exceeds 16 Users
- \* Q174540 Extra Page Printed on Epson Stylus Color Printers
- \* Q174541 Publisher 3.0/4.0 Does Not Print Brick or Vertical Line Patterns
- \* Q174543 Enabling the Shift Lock Feature on Windows NT 4.0
- \* Q174555 STOP 0x0000001E When IIS Service Is Stopped
- \* Q174625 Environment Variables May Prevent Logging On
- \* Q174676 NetWare Authentication Failure When Logging On to NetWare Server
- \* Q174748 XADM: ESEUTIL /g Returns Error -1022
- \* Q174764 Memory Leak in Ntfs.sys
- \* Q174830 NMI Error Message on Blue Screen May Be Garbled
- \* Q174840 Disabling Buttons in the Windows NT Security Dialog Box
- \* Q174844 Spooler Service Causing Access Violation
- \* Q174869 WINS Client Sends Refresh Requests to Secondary WINS Server
- \* Q174871 Printer Shares Lost after Changing Server Name
- \* Q174927 Error Message During Setup of Noncritical Changes
- \* Q174929 No Response to ARP Causes Duplicate IP Addresses on Network
- \* Q174932 STOP 0x0000000A with Halmps.dll When Restarting
- \* Q175035 Diskless Workstations Cannot Find BOOTP Server with DHCP
- \* Q175048 CACLS Quits on Access Denied Errors with /c
- \* Q175093 User Manager Does Not Recognize February 2000 As a Leap Year
- \* Q175225 Disabling Context Menus Does Not Disable Key Combinations
- \* Q175266 Creating Many Partitions Causes Double Drive Letters
- \* Q175321 SNA Client Sessions Hang Until SNA Server Is Restarted
- \* Q175468 Effects of Machine Account Replication on a Domain
- \* Q175637 Poor Print Quality with Epson Stylus Pro XL ESC/P 2
- \* Q175641 LMCompatibilityLevel and Its Effects
- \* Q175643 CR Interpreted As CR/LF When Text Job Is Converted to PCL or PS
- \* Q175667 Error Message: Copy Profile Error
- \* Q175687 Win32k.sys Causes STOP 0x0000001e and 0x0000000a On SMP
- \* Q175738 Collate Feature May Not Work with PostScript Printing
- \* Q175745 Memory Leak When Using Win32 GetClipboardFormat API
- \* Q175877 CSNW Connection Leak When Running 16-bit Applications
- \* Q176081 Access Violation in Explorer.exe Removing a Share
- \* Q176082 RRAS Server Updates Link State Database but Not Route Table
- \* Q176087 LPRMON Status Strings Are No Longer Localized on German Version
- \* Q176209 RAS or RRAS Server Fails to Answer Incoming Calls
- \* Q176211 Console-mode Apps May Run Slowly on Multiprocessor Computers
- \* Q176319 Docfile Standard Marshalling Returns 0x800706f4
- \* Q176322 The Far East GetTextExtent API Fails with Null LPNFit
- \* Q176502 RAS Authentication Rechallenge Resets Compression Flag
- \* Q176922 Multiple IP Addresses Cause Dynamic Packet Filter to Fail
- \* Q176973 Stop 0x0000000A in Netbt.sys on BDC When WINS Server Shuts Down
- \* Q176976 Wrong Return Value from MkParseDisplayName
- \* Q176977 STOP 0x00000023 FAT\_FILE\_SYSTEM with Corrupted Floppy Disk
- \* Q177113 Incomplete Print Jobs Using JetDirect over SPX
- \* Q177125 User Cannot Log On to LAN Because of RAS Logon Failures

UNCLASSIFIED

## UNCLASSIFIED

- \* Q177154 Access Control Causes Reverse Proxy to Fail
- \* Q177245 Multiprocessor Computer May Hang Because of Tcpi.sys
- \* Q177257 STOP 0x0000000A or Difficulty Recognizing IDE CD-ROM Drives
- \* Q177445 Use LoadLibraryEx When Loading Printer Drivers
- \* Q177471 EBCDIC Characters not Properly Converted to ANSI Characters
- \* Q177591 Service Pack Version Truncated in About Box
- \* Q177631 Comdlg32 Fails to Display Drives Mapped by SUBST Command
- \* Q177644 Commenting Macintosh File Changes Date and Time Stamp
- \* Q177647 Nonpaged Pool Size Incorrectly Displayed in Performance Monitor
- \* Q177650 Remote Shutdown Fails If User Is Logged On Without Rights
- \* Q177651 AT Command Handles Quotation Marks Differently
- \* Q177653 CRT Conflict with Getservbyname
- \* Q177654 Slow Network Performance Using NetBEUI Across Bridges
- \* Q177655 Negative Values in Performance Monitor Data
- \* Q177660 Access Violation Occurs in Sfmprint.exe on Busy Print Server
- \* Q177668 Calibration Does Not Change When You Calibrate Foot Pedals
- \* Q177670 RRAS Does Not Enforce Strong Encryption for DUN Clients
- \* Q177676 Stop 0x00000024 May Occur When Bypass Traverse Checking Disabled
- \* Q177677 TSR Applications Hang While Login.exe Is Running
- \* Q177680 With GSNW, WinNT Client Cannot See All Files on NetWare Server
- \* Q177684 Application Using SetOwner May Hang Windows NT User Interface
- \* Q177757 Dr. Watson Does Not Report Service Pack Number
- \* Q177868 SnmpMgrTrapListen API Returns ERROR\_SERVICE\_NOT\_ACTIVE Error
- \* Q177906 Caching Does Not Work Under Reverse Proxying
- \* Q177983 Stop 0xA in Netbt.sys with Greater Than 64 Adapters
- \* Q178109 Roving Profiles for Windows 95 Clients Stop Working
- \* Q178110 FPNW Does Not Allow OS/2 Clients to Open Files
- \* Q178113 Specifying a Group Name in LMHOSTS File May Cause STOP 0xA
- \* Q178202 Fix for Loss of Data Records or Partial Records Written to Disk
- \* Q178205 Connecting to a Server is Slow over RAS Using LMHOSTS File
- \* Q178208 CrashOnAuditFail with Logon/Logoff Auditing Causes Blue Screen
- \* Q178302 XADM: Upgrade to Exchange 5.5 Fails If Virus Software Is Enabled
- \* Q178364 Macintosh Clients See Files on WinNT Server Constantly Moving
- \* Q178381 SNMP Leaks Memory If the OID Cannot Be Decoded
- \* Q178393 SQL Server Hangs When Sending a Message Using SQLMail
- \* Q178413 Windows NT System May Hang When Running a Filter Driver
- \* Q178414 Archive Bit Is Not Reset When a File Is Renamed
- \* Q178471 STOP 0XA Caused by Race Condition in VDM and Process Delete
- \* Q178546 CSNW Does Not Display Directory Name with Extended Characters
- \* Q178550 IP Address Conflict with Address 0.0.0.0
- \* Q178557 Dr. Watson May Display Message Box Even When Disabled
- \* Q178636 Directory Listing Not Correct When Using Russian Characters
- \* Q178723 Problems with "Run Only Allowed Windows Application"
- \* Q178741 Event Log Opening Problem Causes Services.exe Failure
- \* Q179092 NWLNKIPX Sends Broadcast RIPX Packets Over the Network
- \* Q179107 STOP 0x0000000A in Raspppt.sys on a Windows NT PPTP Server
- \* Q179129 STOP 0x0000000A or 0x00000019 Due to Modified Teardrop Attack
- \* Q179147 Access Denied Starting Program
- \* Q179156 Updated TCP/IP Printing Options for Windows NT 4.0 SP3 and Later
- \* Q179157 Stop 0xA in Tcpi.sys When Source Routing Data Exceeds 18 Bytes
- \* Q179187 Problems Using TAPI 2.1
- \* Q179190 NWRDR May Send Excessive GetNearestServer Requests
- \* Q179433 Cache Manager May Cause Data Corruption on SMB Servers on FAT

# UNCLASSIFIED

- \* Q179553 Access Violation in PoEdit When Defining Allowed Windows Apps
- \* Q179741 STOP 0x0A Due to Duplicate Free in Afd.sys
- \* Q179827 Registry Handle Leak Causes Random Blue Screens
- \* Q179873 Files Open with UNC Path May Be Closed Prematurely
- \* Q179983 RDR Sessions on UNC Name Images May Log Off Prematurely
- \* Q179995 Memory Leak in FPNW Causes Windows NT Server to Hang
- \* Q180168 Novell Client 32 for Win95 Displays Duplicate Files on FPNW
- \* Q180356 NWConv Fails to Apply Correct Group Permissions
- \* Q180532 Xircom PC Card Fails to Function
- \* Q180622 STOP:0x0000001E with STATUS\_INSUFFICIENT\_RESOURCES in Sfmsrv.sys
- \* Q180648 Windows NT 4.0 Traps with a Stop 0x24 or Stop 0xA
- \* Q180716 SFM Fails to Accept Associations with Two-Character Extensions
- \* Q180717 SFM: File Date and Time Stamp Change with Get Info
- \* Q180718 SFM: Disconnect Macintosh Clients before Dismounting Volume
- \* Q180854 Access Violation in Winlogon with Third-Party Gina.dll
- \* Q180875 Russian Clients May Have File I/O Problems on an FPNW Server
- \* Q180963 Denial of Service Attack Causes Windows NT Systems to Restart
- \* Q181022 Err: Cannot Write to LPTx Printing to Parallel Port
- \* Q181120 Manual Dial Dialog Fails to Appear when Logging On
- \* Q181311 Data Corruption Occurs with Record Locking on FPNW Server
- \* Q181799 RPC/TCP Connection Attempt Made Only to First Address
- \* Q181859 Stop 0x0000000A When Using UltraBac to Back Up a SQL Server
- \* Q181928 Using POEDIT to Save Policy Files on NetWare Servers May Fail
- \* Q182005 Euro Currency Not Available in Windows NT Character Sets
- \* Q182047 DHCP Server Performance Degraded by Large Number of Scopes
- \* Q182205 Clients Cannot Send Mail Attachments Through Modem Sharing
- \* Q182227 DNS Server Does Not Check for Delegations Before Forwarding
- \* Q182288 RPC May Cause System to Stop Responding during Shutdown
- \* Q182322 SNMP Appends Garbage to Data in Response to SNMP Get
- \* Q182333 Excessive Processor Usage on Print Servers
- \* Q182441 Full Synchronization from WinNT PDC to LanMan Server May Fail
- \* Q182444 NBF MaxFrameSize Calculated Incorrectly on Token Ring
- \* Q182540 WinNT x86 MPS HAL Can Fail To Map System Relative IRQs
- \* Q182644 DNR Sorts IP Address for Multihomed Hosts Before Returning List
- \* Q182781 Client Connections to Multihomed Server Not Load Balanced
- \* Q182816 WINS PriorityClassHigh Parameter Does Not Work After Restarting
- \* Q182817 CSNW: Unable to Rename File on NetWare Server
- \* Q182825 NET USE Returns Error 53 When Host Has 3 or more NICs
- \* Q182918 Account Lockout Event also Stored in Security Event Log on DC
- \* Q183054 Taking Ownership Remotely May Set Owner Incorrectly
- \* Q183069 Ensoniq PCI Sound Card Experiences Static When Disk Is Accessed
- \* Q183123 Find Files Displays Garbled Date if Year is 2000 or Greater
- \* Q183125 Shell Doc Property Dialog Custom Date Incorrect after Year 2000
- \* Q183283 IE Through Proxy Server to IIS May Stop on Page with Scripts
- \* Q183292 Print Preview Frequently Causes Access Violation in Spooler
- \* Q183335 Calling Card and Area Code Not Dialed Using Both TAPI Options
- \* Q183419 Memory Leak in Spoolss.exe Causes Performance Degradation
- \* Q183581 Out of Virtual Memory Messages During Windows NT Installation
- \* Q183651 Default Memory Settings for Lexmark Optra S 1250 Incorrect
- \* Q183652 Access Violation When More Than 200 Adapters Are Installed
- \* Q183653 Client Authentication Fails Connecting to Netscape Server
- \* Q183654 IBM DTTA-351010 10.1 GB Drive Capacity Is Inaccurate
- \* Q183656 XCOPY Returns "Invalid Parameter" When Using Date Switch

UNCLASSIFIED

# UNCLASSIFIED

- \* Q183657 Unable to Insert OLE Objects into Application Documents
- \* Q183664 NDS Logon Scripts Do Not Execute Correctly
- \* Q183676 Window Position of Windisk.exe Causes Access Violation
- \* Q183677 Client Authentication with Personal Certificates Fail
- \* Q183699 Winsdmp.exe Inefficiently Dumps WINS Databases with Large ID
- \* Q183704 Hide Drives Policy in Common.adm Has No VALUEOFF Statement
- \* Q183705 RPC Mishandles Changes in the Number of IP Addresses
- \* Q183709 Printing from Xerox 3006 May Cause Paper Jams
- \* Q183718 CACLS Not Resolving Principle Names Correctly
- \* Q183749 Access Violation in INETINFO:TerminateExtension
- \* Q183755 More Than One Internal IP with Socks Enabled Causes Dr. Watson
- \* Q183812 Problems When a Connection over an ISDN Bridge Is Not Closed
- \* Q183819 DCOM over HTTP Method Calls May Hang for up to 15 Minutes
- \* Q183832 GetHostName() Must Support Alternate Computer Names
- \* Q183840 Stop 0xC000021A When Starting Task Manager with CTRL+ALT+DEL
- \* Q183859 Integrity Checking on Secure Channels with Domain Controllers
- \* Q183875 DHCP Server Leases Excluded Addresses if the Scope Is Expanded
- \* Q183886 Access Violation in LSASS When Logging on System
- \* Q183930 FIX: IP Is Mangled When Using UDP on Multihomed Computers
- \* Q184017 Administrators Can Display Contents of Service Account Passwords
- \* Q184026 NetDDE Causes Dr. Watson When Closing Incomplete Connections
- \* Q184072 HasOverlappedIoCompleted, GetOverlappedResult Give Wrong Value
- \* Q184101 Small Single and Double-Precision Values Are Rounded to Zero
- \* Q184132 Err Msg: Value Entered Does Not Match with the Specified Type
- \* Q184139 Stopping RPC Locator Service Causes Error 2186
- \* Q184213 SystemFileCacheInformation Can Be Changed Without Privilege
- \* Q184219 Access Violation in Microsoft TAPI Browser 2.0
- \* Q184228 Dr. Watson in Nwssvc.exe Deleting Queue and Printer from FPNW
- \* Q184229 Copying Files to a Macintosh Volume Changes Date and Time Stamp
- \* Q184232 DCOMCNFG Saves Incorrect Display Name in Services
- \* Q184278 Server in One Domain May Disconnect Client in Another Domain
- \* Q184288 GP Fault May Occur with IIS on Multi-processor System
- \* Q184344 Reconcile on DHCP Scope Does Not Work Correctly for BOOTP Client
- \* Q184350 WordPerfect Suite 6.0 Setup Fails with Multiple CD-ROMs
- \* Q184353 DHCP ALT+H Shortcut Key for HELP Is Not Available
- \* Q184414 Access Violation When Printing PostScript to SFM Print Server
- \* Q184537 Very Large Files Cause Performance Problems
- \* Q184538 Error Message: A Controller for This Domain Could Not Be Found
- \* Q184744 DHCP Server Leaks Registry Quota on Alpha Version of Windows NT
- \* Q184752 Xerox PCL Does Not Print Landscape
- \* Q184754 Several Threads Created in LRPC Running Stress Test in IIS
- \* Q184758 STOP 0x78 When NonPagedPoolSize > 7/8 of Physical Memory
- \* Q184794 STOP 0x50 May Be Caused by PPTP Registry Entries
- \* Q184832 Intermittent Name Conflicts with WINS Server
- \* Q184835 Explorer on Windows 95 DFS Client May Hang
- \* Q184836 Application Access Violates When Session Is Terminated
- \* Q184875 API Function BroadcastSystemMessage() Always Returns 1 (Success)
- \* Q184879 Windows NT Logon Dialog May Disappear
- \* Q184881 Reverse Lookups with BIND Earlier Than 4.8.3 Fail
- \* Q184891 Server.HTMLEncode Garbles Extended Characters
- \* Q184937 Session Between Multihomed Computers May End Unexpectedly
- \* Q184954 Computer Hangs While Booting with HP 6L Printer out of Paper
- \* Q184996 Incomplete List of NetWare Server Volumes with CSNW/GSNW

# UNCLASSIFIED

- \* Q184998 RDR May Read or Write from Wrong File If File Is Memory Mapped
- \* Q185051 Restarting Cluster Service Causes Services.exe to Crash
- \* Q185081 No Domain Controllers Found When Logging on Using RAS
- \* Q185137 Log Logical Record Request May Be Sent to Wrong Server
- \* Q185142 NetWare API Log Logical Record May Incorrectly Succeed
- \* Q185203 SPOOLSS Hangs When Printing a File With a Corrupted EMF Record
- \* Q185212 Cluster Server Does Not Support More than 900 Shares
- \* Q185219 IIS 4.0 with Multiple Certificates May Return Error
- \* Q185260 User Accounts May Get Locked out After Entering Wrong Password
- \* Q185300 STOP 0x24 in Ntfs.sys Function NTFSMoveFile()
- \* Q185323 Pool NonPaged Bytes Not Accurately Calculated for User Mode
- \* Q185349 Problems Remotely Accessing W3 or FTP Perfmon Counters
- \* Q185355 Printers Folder Displays Printer Error When Printer Is Busy
- \* Q185559 Negative Value in NtGdiFastPolyPolyline Causes Blue Screen
- \* Q185568 WlxCloseUserDesktop Function Unavailable for GINA Writers
- \* Q185571 Printing from Lotus Freelance 97 Produces Thin Horizontal Line
- \* Q185605 Stop Error Caused by Invalid Use of Private Video Driver Handle
- \* Q185624 Calls to NtQueryVolumeInformationFile May Cause Stop 0x0000001E
- \* Q185625 Windows NT Client Logon Fails with EnableSecuritySignature Set
- \* Q185668 IntelliMouse TrackBall Wheel Does Not Work with Service Pack 3
- \* Q185682 Bugcheck When IPX Is Bound to Only Ndiswan Adapter
- \* Q185722 SFM Rebuilds Indexes upon Restarting of Windows NT
- \* Q185723 Explorer File Copy from Windows 95 Share Fails
- \* Q185727 BUG: closesocket() Fails with 10038 After \_open\_osfhandle()
- \* Q185729 Computer Becomes Unresponsive During CGI Stress Test
- \* Q185734 DNS Server Access Violation in Dns!sendNbstatResponse Routine
- \* Q185735 Explorer Crashes When Dragging Lotus Notes Files over Toolbar
- \* Q185736 Applications May Appear Hung or Unresponsive on Windows NT 4.0
- \* Q185765 HP LaserJet 4Si Driver Unprintable Region is Incorrect
- \* Q185773 NTFS Corruption on Drives > 4 GB Using ExtendOEMPartition
- \* Q185787 STOP 0x0000002E on Alpha with ISA Sound Card
- \* Q185788 Windows NT Hangs on Boot on DEC Alpha Clustered Servers
- \* Q185791 STOP on DEC Miata and Rawhide Platforms Using Graphics Tablet
- \* Q185867 STOP 0x0000000A in Win32k.sys After Installing Korean Office 97
- \* Q185870 IIS: SQL Server Insert Error Regarding Column Name Mismatch
- \* Q185892 Unwanted Popup Message While Printing to an LPR Printer
- \* Q185944 Stop 0x7B After Installing Windows NT on an ALR Evolution-V ST
- \* Q185945 Access violation in win32k!HMMarkObjectDestroy in JPN and KOR NT
- \* Q186051 Archive Bit Is Not Set with File or Directory Rename
- \* Q186078 Name Resolution May Fail If NetBios Name Has ASCII Character
- \* Q186081 STOP 0x0000000A When Restoring Tape
- \* Q186101 FTP Client Does Not Show the Correct Transfer Size for Files
- \* Q186150 NetBEUI May Hang When Using Arcnet Under Heavy Network Traffic
- \* Q186158 Blue Screen When Shutting Down with RAS Connection Established
- \* Q186217 3C509 Is Not Autodetected During Setup on ThinkPad 760EL & XL
- \* Q186241 Dr. Watson May Cause CPU Usage to Spike
- \* Q186247 Users Are Unable to Print to Server
- \* Q186339 Adobe ATM 4.1 OpenType Fonts Not Showing up in Font Menu
- \* Q186357 RPC UseWinsockForIP is Only Applicable to UDP and IPX
- \* Q186416 System Hang Results from Large Number of Notify Syncs
- \* Q186434 Slow Network Default Profile Operation
- \* Q186439 Removing Server Service Results in Memory Leak
- \* Q186455 Mgmtapi.dll Opens Trap Socket in Exclusive Mode

UNCLASSIFIED

# UNCLASSIFIED

- \* Q186463 Windows NT Replies to Address Mask Requests
- \* Q186473 You Can Delete All Records on a WINS Server Using SNMP
- \* Q186494 Event ID 517 Not Created When Security Log Is Cleared
- \* Q186495 WOW Leak Launching Many Instances of a 16-Bit Application
- \* Q186669 FPNW Logout.exe Incorrectly Reports Year After Jan. 1, 2000
- \* Q186743 International Characters Print Incorrectly in Schedule Plus
- \* Q186746 International Calling Codes Updated in Service Pack 4
- \* Q186770 Windows NT Hangs Trying to Access SuperDisk SLS-120 Disk Drive
- \* Q186805 Intermittent Stop 0xA in Srv.sys on Shutdown
- \* Q186820 DNS Server Returns Wrong Response When WINS Lookup Is Enabled
- \* Q186860 Update Memory Settings and Add Exec Paper Size to Sharp Models
- \* Q186873 Netbios Delays Sending/Receiving Packets When Session Is Lost
- \* Q186904 MPROUTER Access Violation on Invalid Radius Response
- \* Q186905 Radius Client Uses 100 Percent CPU on Invalid Response
- \* Q186929 LowercaseFiles Registry Key Has Added Functionality
- \* Q186963 Incorrect Dimensions in Executive Form with Mannesmann Driver
- \* Q187277 The FTP PORT Command Fails in IIS 3.0
- \* Q187302 Stop 0x00000040 in NetBT Protocol
- \* Q187392 PATCH: Stop 0x0000000A in Wind32k.sys xxxDDETrackWindowDying
- \* Q187493 Some Netscape Client Certificates Rejected by IIS
- \* Q187508 FTP Server Fails to Respond If First Binding Does Not Work
- \* Q187518 Apps Using Beep API on Multiprocessor Systems May Crash
- \* Q187519 NTBackup Will Not Run from Command Line with Blank Space
- \* Q187520 Tandberg SL5 Tape Device Not Auto-Detected in Window NT 4.0
- \* Q187555 WINS Incorrect Version ID Assigned During Scavenging
- \* Q187576 Stop 0x0000000A May Occur in TCP/IP
- \* Q187577 STOP 0xA Because of Spin Lock in Sfmatalk.sys on DEC Alpha
- \* Q187615 Setup Hangs When System Includes More Than Two RAW Drives
- \* Q187669 Unable to Use NetBIOS Resources over SLIP
- \* Q187672 Access Violation in RAS Using Multilink
- \* Q187686 LookupAccountSid Causes Access Violation on Multihomed System
- \* Q187696 Changes to Calculator in Service Pack 4
- \* Q187705 Application Error in CoreIWEB.GALLERY
- \* Q187708 Cannot Connect to SQL Virtual Server via Sockets in Cluster
- \* Q187709 Domain Name Resolver Caches Responses
- \* Q187769 Application Error in NTVDM Running cc:Mail Utilities
- \* Q187802 DHCP Assigns "Bad\_Address" to "Host Unreachable"
- \* Q187830 Performance Decrease Transmitting Data over the Network
- \* Q187856 IIS: Limit SSL Message Size to 16 KB for Netscape
- \* Q187884 CoCreateInstance on Multiple Threads Causes Hangs or Failures
- \* Q187936 Application May Hang Calling LogonUser() API
- \* Q187939 IPX May Not Work When Packet Size Is Larger Than Receive Buffer
- \* Q187940 Input Filters over IPX WAN Routing May Fail to Filter Packets
- \* Q187941 An Explanation of the New CHKDSK /C and /I Switches
- \* Q187947 100 Percent CPU System Handle Problem
- \* Q187964 MGI PhotoSuite May Paste Screenshots as Garbage or an AV Occurs
- \* Q187999 "Access Denied" w/ Personalization & Membership Authentication
- \* Q188000 Cannot Enter Stand-Alone Dieresis Character on Swiss Keyboards
- \* Q188027 Performance, Audit Logging, and Fixes to the DHCP Service
- \* Q188303 Random Stop 0x50 Errors on Cirrus Video Adapters
- \* Q188312 Lexmark Optra E+ Unprintable Region Is Incorrect
- \* Q188315 Stop Error Message in Sfmsrv.sys
- \* Q188414 Random Stop 0x0000000A When Running IPX over Token Ring

# UNCLASSIFIED

- \* Q188424 Multilayered Display Driver Produces Black Line in Word
- \* Q188571 STOP 0x0000000A in Netbt.sys Caused by Invalid DNS Record
- \* Q188652 Error Replicating Registry Keys
- \* Q188700 Screensaver Password Works Even if Account Is Locked Out
- \* Q188806 "::\$DATA" Data Stream Name of a File May Return Source
- \* Q188838 Task Manager CPU Usage Only Displays Eight Processors
- \* Q188879 RPC Endpoint Mapper Will Not Register All Interfaces
- \* Q188896 Access Violation in Explorer.exe Changing Share Permissions
- \* Q189010 SBS: RAS Leases Six Addresses from DHCP
- \* Q189011 Using Performance Monitor Remotely Causes Access Violation
- \* Q189012 Clicking Default Scope Does Not Open Active Lease Window
- \* Q189013 Atapi.sys Does Not Support Multiple Logical Devices
- \* Q189032 Floating Point Arguments Won't Pass Between NT RPC and IBM RPC
- \* Q189061 Repeated Regsavekey/Regstorekey Actions Corrupt Registry Hive
- \* Q189080 TCP Connection May Drop When Transferring Large Amounts of Data
- \* Q189114 NetDDE Refuses Incoming WM\_DDE\_INITIATEs from Windows 95
- \* Q189119 UserEnv Returns Corrupted Profile for All Failures
- \* Q189171 WinSock Applications May Fail or Stop Responding
- \* Q189225 LMMIB2 Unable to "Walk" from .1.3.6.1.4.1.77.1.4.4
- \* Q189245 Lmmib2.dll Does Not Support All Objects
- \* Q189262 FTP Passive Mode May Terminate Session
- \* Q189276 ODBC Causes Access Violation in 16-Bit Winsock
- \* Q189283 No More Than About 570 Reservations Visible in a DHCP Scope
- \* Q189290 Loss of Desktop After Logon When Using a Filter Gina.dll
- \* Q189291 Hang in Winlogon on Workstation Locked Dialog Box
- \* Q189395 Support for Canadian ACNOR Keyboard
- \* Q189462 Only Partial Pages Displayed or Error "The Connection Was Reset"
- \* Q189471 WpuOpenCurrentThread Does Not Work
- \* Q189522 Network Drive Letters in PATH Statement Causes Excessive Traffic
- \* Q189579 F11 and F12 Keys Do Not Function in MS-DOS Applications
- \* Q189606 Browser Service Fails to Start or Stop Button Is Unavailable
- \* Q189612 Access Violation Occurs in Windows NT Explorer (Explorer.exe)
- \* Q189756 PerfMon Percentage of Registry Quota in Use Displayed Wrong
- \* Q189988 CMPXCHG8B CPUs in Non-Intel/AMD x86 Compatibles Not Supported
- \* Q190009 Client Cert. Mapping Only Works w/First Page on Proxy Connection
- \* Q190010 Logging Performs Unwanted Flushes of Log Data Buffer
- \* Q190011 Perl Script Mappings Converted to Uppercase During Upgrade
- \* Q190015 Setting LogonMethod to Batch Causes "Parameter is Incorrect"
- \* Q190288 SecHole Lets Non-administrative Users Gain Debug Level Access
- \* Q190354 Unattended Setup of MSCS with -JOIN Parameter Requires Input
- \* Q190449 Corrupted SAM Hangs Windows NT Server
- \* Q190506 WINS Replication Problem Events 4262, 4261, and 1c Replication
- \* Q190552 WinNT 4.0 DHCP Client Modified to meet RFC 2131
- \* Q190791 STATUS\_CANT\_WAIT Returned from an NtCreateFile Call
- \* Q190834 SCSI Adapter Is No Longer Visible from SCSI Adapters Utility
- \* Q190928 Poedit Spin Boxes Limit Max Value to 9999
- \* Q190931 Snpmptrap.exe Ignores SNMP Trap PDU Greater Than 4,096 Bytes
- \* Q190932 SNMP Service Ignores SNMP Trap PDU Greater Than 4,096 Bytes
- \* Q191088 Printer Prompts for Paper with Dutch Workstations
- \* Q191098 Large File Copy Operation Causes Available Bytes to Drop
- \* Q191284 STOP 0x0000001E in Netbt.sys
- \* Q191285 Services for Macintosh Index Corruption on Large Volumes
- \* Q191309 ALT+Numeric Keypad Problem When CHCP Command is Used

UNCLASSIFIED

# UNCLASSIFIED

- \* Q191362 FPNW Pass-Through Authentication from Trusted Domain May Fail
- \* Q191387 Unable to Run 16-bit Apps If FILES= Is Greater Than 255
- \* Q191418 Arcs Print Incorrectly with EMF on PCL Printers
- \* Q191419 GP Fault or Access Violation When Buffer Too Small
- \* Q191428 WINS Replication Fails If More Than 30 Partners Are Configured
- \* Q191614 Able to Commit More Memory Than Is Available
- \* Q191634 Group Policies Cause Excessive \PIPE\samr Connections on PDC
- \* Q191689 Incorrect Font Characteristics May Be Used on Imported Graphics
- \* Q191751 Smoothing Fonts Disabled Using ETO\_GLYPHINDEX
- \* Q191756 Stop 0x1E Switching Between System Menus in Application Window
- \* Q191767 LogicalDisk Partition Missing in Performance Monitor
- \* Q191768 Date of Print Job May Be Displayed Incorrectly in Print Queue
- \* Q191775 WINS Service Fails to Start With More Than 99 PNG Entries
- \* Q191830 Memory Leak Due to Repeated Logon/Logoff May Corrupt Profiles
- \* Q191832 Access Violation in Hangul Version of Lotus Organizer 97
- \* Q191834 Network Problems That Occur When Logging Off May Corrupt Profile
- \* Q191850 Convert Reports Cannot Create Elementary File System Structures
- \* Q191852 Bhnetb.dll Leaks Memory in Winlogon.exe Process with NetMon
- \* Q191896 Printing to NT LPD Server from SUN OS 4.1.4 May Not Process C/R
- \* Q191915 Screen Saver Time-out is Limited to 60 Minutes
- \* Q191992 NdrConvert Causes Access Violation in RPC Client on WinNT 4.0
- \* Q192051 LDAP Does Not Authenticate on French WinNT Due to Encryption
- \* Q192056 Point and Print Functionality with More Than 20 Driver Files
- \* Q192104 Windows NT Does Not Start If Primary Partition Is Above 2 GB
- \* Q192126 Add Workstation Fails with RestrictAnonymous
- \* Q192127 BUG: RpcTestCancel() Always Returns Error Code 5
- \* Q192132 STA Threads Lose Thread Token
- \* Q192229 Login Script Group Membership Mapping on BDC Fail If PDC Is Down
- \* Q192266 Sockets-based Child Processes Are Not Stopped
- \* Q192267 Various STOP Errors When Opening Files on Novell NetWare Servers
- \* Q192293 IIS Stops ODBC Logging after Failing to Communicate with SQL
- \* Q192409 Open Files Can Cause Kernel to Report INSUFFICIENT\_RESOURCES
- \* Q192453 MoveFile API from Windows 95 with Invalid UNC Causes STOP 0xa
- \* Q192457 Downloaded File May Be Saved in Incorrect Folder with IE
- \* Q192460 Matrox Video Driver Causes STOP 0x00000050
- \* Q192547 WINSADMIN Writes Invalid SP Time to Registry
- \* Q192690 Search: Unable to Connect to Catalog Server via Search MMC
- \* Q192736 STOP 0x0000000A Blue Screen on Alpha AXP
- \* Q192749 Multiple SSL Connections May Cause Error Starting Security Sys
- \* Q192774 Stop 0x0000000A in Tcpip.sys Processing an ICMP Packet
- \* Q192786 Event ID 11 Changed to an Informational Message
- \* Q193056 Problems in Date/Time after Choosing February 29 in a Leap Year
- \* Q193064 Pressing Cancel Button in Date/Time Utility Changes Date
- \* Q193090 Inetmib1.dll Causes Memory Leak in Winlogon.exe Process
- \* Q193106 Filesystem Filter Drivers may Unload Unexpectedly
- \* Q193121 Cannot Connect to DFS Leaf a Second Time if Server is NetWare
- \* Q193157 TCP/IP Does Not Allow MAC Addresses to Change Dynamically
- \* Q193169 Script Mappings Are Not Removed from the Registry after Migration
- \* Q193206 Acquiring SNMP Info For OSPF in RRAS Hangs
- \* Q193209 Gethostbyname Not Working Correctly with Only DUN Installed
- \* Q193233 Rpcs.exe Consumes 100% CPU Due to RPC Spoofing Attack
- \* Q193271 Cannot Create Virtual Directory in Administrator Program
- \* Q193371 WINS/DHCP Admin Show Expiration Dates 2000 - 2009 with One Digit

# UNCLASSIFIED

- \* Q193436 DHCP Client Shuts Down After Two Declines
  - \* Q193499 Multiple RRAS Client Disconnects Cause Increased CPU Usage
  - \* Q193525 Access Violation Occurs When Viewing Web Sharing Tab
  - \* Q193526 W3SVC Counters Fail after a Successful Install
  - \* Q193528 Internet Service Manager Does Not Allow Wildcard Redirections
  - \* Q193529 Modem Sharing Clients Cause Stop 0x000001E on SBS
  - \* Q193530 Access Violation in WINSCL When Using CR or SDB Parameter
  - \* Q193532 Stop 0x0000000A When Running Executable from Floppy Disk
  - \* Q193548 Stop 0x0000002E Using Qlogic Driver Version 2.29
  - \* Q193596 RASMAN Registry Values Cannot Be Set Higher Than 0xFF
  - \* Q193613 ADSI Paths Greater than 80 Characters Causes Access Violation
  - \* Q193614 Viewing Computer from MMC Causes Access Violation to Occur
  - \* Q193646 Event ID 10005 from DCOM After Installing IIS
  - \* Q193654 Services Continue to Run After Shutdown Initiated
  - \* Q193655 Multiple Entries for AUTOCHK Abort in System Log
  - \* Q193686 SMTP Services Do Not Start Automatically After One Is Stopped
  - \* Q193687 Invalid Handle Exception Error During SMTP Server Maintenance
  - \* Q193688 HTMLA: Object Already Exists When Creating New Web Sites
  - \* Q193689 IIS Security: Mapping IDC Reveals Paths for Web Directories
  - \* Q193779 Cluster Server Drive Letters Do Not Update Using Disk Admin
  - \* Q193781 Cache Manager May Cause Data Corruption
  - \* Q193793 "::\$DATA" Data Stream Name Returns Source of a Remote File
  - \* Q193806 CSNW Error 85, Local Device Already in Use
  - \* Q193812 Extended Characters in URL Translated into UTF-8 Characters
  - \* Q193891 HTTP Through Firewall and "Bypass Proxy for Local Intranet"
  - \* Q193899 Event ID 1008, 4005 with Missing TCP/IP Performance Counters
  - \* Q194130 SNMP Edit Box Drops a Character When Writing to the Registry
  - \* Q194133 Remote Shell (RSH) Commands Hang w/ Multiple Sessions Running
  - \* Q194193 STOP 0xA in Sfmataik.sys When Copying Files on an SFM Volume
  - \* Q194194 DNS Fails with Error 1201 If Secondary Zone File Not Specified
  - \* Q194200 Cannot Change WinNT Passwords from Exchange and Outlook Clients
  - \* Q194228 Rule Containing Multiple Clauses Only Functions Properly Once
  - \* Q194322 T/R NIC May Fail Windows Hardware Quality Lab (WHQL) Test
  - \* Q194336 ERROR: Destroyed NTFS Directory
  - \* Q194340 Access Violation when Using Rcp.exe to Copy to Unix
  - \* Q194341 Simple TCP/IP Services Can Be Driven to 100% CPU
  - \* Q194393 New Window From Here Option in MMC May Cause Fatal Error
  - \* Q194424 DHCP Server May Fail to Record Lease
  - \* Q194429 TCPIP Timewaitstate may not remain in 2\*msl
  - \* Q194431 Applications May be able to "Listen" on TCP or UDP Ports.
  - \* Q194465 PPTP May Refuse Connections When VPNs Are Free
- Service Pack 3
- \* Q135707 Programs Run at Priority Level 15 May Cause Computer to Hang
  - \* Q139506 Connections to Share-Level Server May Fail
  - \* Q140419 Name Release Notifications Not Sent to WINS on Shut Down
  - \* Q140967 Changing Password in User Manager Does Not Permit Logon
  - \* Q141189 BUG: Wrong Error Code on NetBIOS Call When Using NWNBLNK
  - \* Q141381 Retail SP3 Clients Cannot Connect to SP3 Beta 1 Servers
  - \* Q142047 Bad Network Packet May Cause Access Violation (AV) on DNS Server
  - \* Q142609 Corruption Problem When Running DPMI Application
  - \* Q143470 Run Logon Scripts Synchronously Not Applied to New Users
  - \* Q143472 FPNW Blue Screens Accessing or Creating Folders with Long Paths
  - \* Q143473 Unattended Setup Stops Unexpectedly

UNCLASSIFIED

# UNCLASSIFIED

- \* Q147012 Activating /W Switch to Prevent Rebooting in WinNT
- \* Q149538 System Restarts Every 5 Hours if Workstation to Server Upgrade
- \* Q151926 Delayed WinLogon When Drive Mapped to Local Share
- \* Q152273 DHCP Server May Give Out Duplicate IP Addresses
- \* Q153220 DHCP Manager Error "No More Data Is Available"
- \* Q154710 Cannot View Long File Names on Network in 16-Bit Programs
- \* Q154939 CreateQueueJobAndFile Fails w/ Queues Other Than Print Queue
- \* Q156410 STOP 0x1E or 0x50 Error on Multiprocessor DEC Alpha Computer
- \* Q157077 Netstat Slow to List Large Numbers of Connections
- \* Q157745 Command Extensions Cause Access Violation in Cmd.exe
- \* Q158433 Re-creating Admin Shares Causes Exception Error
- \* Q158548 Sysdiff Changes Dates on Files It Applies to WinNT
- \* Q159060 Mouse Cursor Freezes or Fails with Microsoft IntelliMouse
- \* Q159176 XADM: Store Stops Responding with High CPU Usage
- \* Q159330 Map.exe Does Not Set Environment Variables Correctly
- \* Q159998 Error Message: Error Access Is Denied
- \* Q160386 Incorrect MediaType Parameter on IBM PCMCIA Token Ring Card
- \* Q160405 Video Memory Not Correctly Detected on Dell Latitude Laptops
- \* Q161038 Winsock Apps Fail on First Attempt at NetBIOS Name Resolution
- \* Q161368 Service Pack 2 May Cause Loss of Connectivity in Remote Access
- \* Q161432 WINS Static Entries Overwritten by Duplicate Group Names
- \* Q161644 STOP 0x0000000A Sfmsrv.sys When Copying File to Mac Volume
- \* Q161714 IPX Doesn't Function Correctly over Token Ring Source Routing
- \* Q161830 Message from Unix Using Smbclient w/ Long Username Crashes
- \* Q161838 Programs That Lock 0 Bytes at Byte 0 Lock Entire File
- \* Q162077 Stop: 0x0000000A when Selecting NDS Map Objects
- \* Q162096 SET: Drivers Fail to Load When I/O Address Is Above 0xFFFF
- \* Q162189 Macintosh Clients May Hang Temporarily with Multiple Mac Volumes
- \* Q162396 Problem with DHCP Decline Feature in Service Pack 2
- \* Q162404 Service Pack 5 Breaks Microsoft Mail Shared Using FPNW
- \* Q162471 Windows NT 4.0 May Not Recognize SCSI Devices Using Nonzero LUNs
- \* Q162563 WINS Restore Fails on Windows NT Server 4.0
- \* Q162566 FPNW Causes Incomplete Display When Executed from Windows 95
- \* Q162567 Telnet to Port 135 Causes 100 Percent CPU Usage
- \* Q162616 Extra Form Feed with Passthrough Functions to Text Only Driver
- \* Q162657 Choosing Default Domain Name for RAS Client Authentication
- \* Q162774 Policy Editor Crashes When Using Large Custom ADM Files
- \* Q162775 Access Violation in SPOOLSS when Printing to a Serial Printer
- \* Q162778 WINS May Report Database Corruption w/ More Than 100 Owners
- \* Q162881 RIP Table Sent While Shutting Down When Silent RIP Set
- \* Q162926 STOP: 0x0x0000000A After Call to GlobalAddAtom()
- \* Q162927 Telnetting to Port 53 May Crash DNS Service
- \* Q163129 RAS Client Fails to Connect to Service Pack 2 Using NetBEUI
- \* Q163143 STOP: 0x0000001E with Status C000009A
- \* Q163196 New Windows NT PING.EXE Prevents Hanging Other TCP/IP Stacks
- \* Q163202 Limit of the Number of Simultaneously Open Root Storage Files
- \* Q163203 Remote Access Autodial Manager may fail for second user logon
- \* Q163213 WebSTONE Benchmark of IIS May Show Poor Results for MP Systems
- \* Q163214 RAS Script with Set IPADDR May Fail with 3Com Defender Add-on
- \* Q163261 DEC ALPHA WinNT 4.0 Servers w/ SP2 Fail to Lease DHCP Addresses
- \* Q163267 Delay While Establishing SPX II Connection
- \* Q163318 Helpfile Word Lists May Be Rebuilt After Daylight Savings Change
- \* Q163333 Autosynch Compatible COM Applications May Fail w/ FIFO Enabled

# UNCLASSIFIED

- \* Q163383 Failure to Obtain IP Address Via DHCP on Token Ring w/ SP2
- \* Q163431 16-Bit Application Stops Responding When Run on WinNT 4.0
- \* Q163508 STOP 0xA in Ntfs.sys During Reboot
- \* Q163512 Error: The Mapi Spooler has Shut Down Unexpectedly
- \* Q163525 Delay When Saving Word 7.0 File to Windows NT 4.0 Server
- \* Q163538 NTBackup Does Not Properly Eject Tapes on DLT Tape Devices
- \* Q163614 HP LaserJet Series II Prints Extra Small Stripes or Points
- \* Q163616 Cannot Unlock Workstation If Password Change Cancelled
- \* Q163620 STOP 0x50 in Rdr.sys If Pathname Too Long in SMB
- \* Q163672 Windows NT 4.0 Setup Fails on ThinkPad 535
- \* Q163687 Winsock Applications May Timeout or Fail with an Error
- \* Q163700 IIS Access Violation for Polygon with More Than 100 Vertices
- \* Q163714 ATDISK Finds the Same Disk Twice on SunDisk PCMCIA ATA Adapter
- \* Q163725 NDIS Driver Fails To Check Functional Address
- \* Q163790 RPC Service Stops Responding on UDP Port 135
- \* Q163872 Sysdiff Cannot Delete Files
- \* Q163873 Czech Keyboard Layout Has Wrong Mapping
- \* Q163874 Pressing CTRL+ALT+DEL When Logging On Can Cause Blue Screen
- \* Q163875 Group Policies Not Applied If DC Name Is More Than 13 Characters
- \* Q163876 CSNW Clients Cannot Delete Print Jobs on NetWare Print Queue
- \* Q163880 COPY Command Causes File Cache to Grow
- \* Q163881 Windows NT Does not Display Some Fonts
- \* Q163883 NetBT (tag=Nbt8) Corrupts Pool with WinNT 4.0 SP2 Installed
- \* Q163891 Microsoft Excel 97 Causes a Windows NT Access Violation
- \* Q163892 A Service May Not Set Hooks on 32-bit GUI Applications
- \* Q163936 CLOCK Hangs and Consumes 90% CPU When Set to Digital Display
- \* Q163969 Event 552: DNS Was Unable to Serve a Client Request
- \* Q164014 Slow Exchange Client Logons Due to Deadlock in LSASS
- \* Q164121 Corel Fonts Unavailable Outside of English Locale
- \* Q164133 Logon Allowed When Access Denied to Mandatory User Profile
- \* Q164138 Files in Macintosh Volume Disappear from Macintosh Clients
- \* Q164159 Verify Reports Errors When Restoring a Tape Backup
- \* Q164161 NTBACKUP Fails to Back up Microsoft Exchange Server Data
- \* Q164201 Access Violation Installing IIS
- \* Q164211 FPNW Doesn't Convert the Long File Names Correctly
- \* Q164260 Compressing and Uncompressing Files Cause File Cache to Grow
- \* Q164309 Windows NT Client: Primary/Secondary WINS Servers Switch
- \* Q164322 Memory Leak in NetQueryDisplayInformation API
- \* Q164350 NEC IDE CD-ROM Drive CDR-1400C Cannot Play Audio CDs
- \* Q164352 Stop 0x00000050 in Tcpi.sys Caused by Winsock Applications
- \* Q164391 WinNT 4.0 SP2 Atapi Claims IRQ for Unused IDE Channel
- \* Q164410 CHGPASS and SETPASS Do Not Prompt For Typing Correction
- \* Q164432 Accented Greek Characters Are Not Being Created
- \* Q164462 Conner 4 mm DAT Tape Devices Fail After About 30 Seconds
- \* Q164491 Stop: 0x0000000A in Rdr.sys When Mailslot Message > 512 Bytes
- \* Q164507 Any User Can Log on to FTP Server with Disabled Anonymous Logon
- \* Q164542 MGET to an IBM Host FTP Server Returns Garbage Characters
- \* Q164546 SCSI Driver Description Truncated in Control Panel
- \* Q164595 Duplicate Route Not Removed After Second Redirection
- \* Q164600 4 mm DAT Driver Reports DEC TZ9L Supports Setmarks
- \* Q164606 Deferred Reconnections to Password Shares May Not Work
- \* Q164630 RPC over NetBEUI Fails from WinNT 4.0 RAS to WinNT 4.0 RAS
- \* Q164631 Scavenging WINS Database Removes Static Entries

UNCLASSIFIED

# UNCLASSIFIED

- \* Q164639 SNA Windows 95 Fails Logon If Password Change Required
- \* Q164702 WINDISK crashes during initialization when Compaq ATAPI PD/CD
- \* Q164758 Remote Procedure Call (RPC) Service Access Violation
- \* Q164806 CHKNTFS Does Not Exclude FAT Partitions from AUTOCHK on Boot
- \* Q164812 Computer Name Truncated When Name Resolution Attempted
- \* Q164821 DHCP Server Service May Stop Responding
- \* Q164826 Direct Draw Programs May Hang NT 4.0 with S3 968 Video Chipset
- \* Q164904 Stop 0x0000000A in NETBT.SYS After Applying Service Pack 2
- \* Q164928 Not All Objects Are Displayed When Browsing NDS Trees
- \* Q164938 Event Logging Frozen While Doing Heavy Logging; Services CPU Peg
- \* Q164982 Lack of Secondary Address May Cause DNS Service to Hang
- \* Q164987 Hard-coded Socket of 451 Causes LANtegrity Software to Fail
- \* Q165004 NTVDM Support for Compaq Financial Keyboard Scan Codes
- \* Q165245 DDE Client Experiences Intermittent DDE Disconnects
- \* Q165314 Grace Logon Remaining Is Not Decrementated When Logging to BDC
- \* Q165388 Invalid Directory Returned When Attempting to Access FPNW
- \* Q165427 Convlog.exe May Cause Access Violation
- \* Q165443 NDS Login Script Fails When Checking "If Member Of"
- \* Q165456 STOP 0x0000000A in Ntoskrnl.exe
- \* Q165483 RasEnumEntries() API Leaks Memory
- \* Q165813 16-bit Applications Cause Access Violation in NTDLL.DLL
- \* Q165814 Stop: 0x0000001E When Opening My Computer
- \* Q165816 STOP 0x0000000A in HAL.DLL on Multiprocessor Computers
- \* Q165818 Truncation of Backup Log In Eastern Europe or Russian NT 4.0
- \* Q165946 RasEnumEntries Return Incorrect Number of Phonebook Entries
- \* Q165950 Unable to Change Font Cartridge Selection
- \* Q165989 GetPeerName() Returns WSAENOTCONN After Select() Returns Success
- \* Q166043 DHCPAdmin Incorrectly Writes the BootFileTable in the Registry
- \* Q166148 RasSetEntryProperties() Fails to Set Options in Service Pack 2
- \* Q166158 Access Violation Occurs in SPOOLSS.EXE
- \* Q166159 Connecting to Windows Network resources from multi-homed machine
- \* Q166183 FPNW Server Returns Error When User Opens More Than 256 Files
- \* Q166186 OS/2 with TCP\IP May Refuse Socket Connections from Windows NT
- \* Q166197 NBTSTAT Error when Using >25 Dialout Devices with RAS
- \* Q166222 Dlc.sys Sends Frame Reject (FRMR) and Drops Connection
- \* Q166224 SNA Server 802.2 Connection Fails to Reactivate
- \* Q166226 Backup of Local Registry Does Not Work With NTBACKUP.EXE /b
- \* Q166257 Applications Using OpenGL Cause Access Violation in OPENGL.DLL
- \* Q166265 Printing To A Postscript Printer May Cause A STOP 0x0000003b
- \* Q166266 STOP 0x0000000A Using OpenNT Commands and Utilities
- \* Q166267 Office Shortcut Bar Fonts Appear as Non-Cyrillic on Russian NT
- \* Q166311 Memory Leak Retrieving OLE Property Values with Service Pack 2
- \* Q166334 OpenGL Access Violation on Windows NT Version 4.0
- \* Q166421 FPNW Returns Time Stamp with 60 Seconds to Clients
- \* Q166423 Access Violation in SERVICES.EXE in EVENTLOG.DLL
- \* Q166475 NWLNKSPX Retransmission Problem Over a Slow Link
- \* Q166478 Logon Rights Are Not Audited
- \* Q166482 DUMPCHK.EXE Incorrectly Reports Some Dump Files as Invalid
- \* Q166686 RASDIAL Error w/English Text on Non-English Version of Windows NT 4.0
- \* Q166696 NT 4 Err Msg: "The INF OEMNADDI is missing the referenced file"
- \* Q166823 Cannot Connect To AT&T Advanced Server VMS or OSF Print Share
- \* Q166834 Lost Record Locks from MS-DOS-based Program to NetWare Server

# UNCLASSIFIED

- \* Q166842 CSNW & GSNW Won't Display NetWare Servers via a SAP Seed Server
- \* Q166846 Cannot Reconnect to TN3270 Server with Close Listen Sockets
- \* Q166874 No Crashdump and Compaq Systems with Smart-2/P (PCI) Controller
- \* Q166963 Cannot Communicate with Computer Running NWLink IPX/SPX
- \* Q166964 Incorrect File Listing on NetWare Server with DIR /TC Command
- \* Q167009 Description of DHCP Server Service Has a Misspelled Word
- \* Q167010 Access Violation in CMD.EXE Processing Batch File Script Argument
- \* Q167026 Windows NT 4.0 DNS Server Stops Responding To Queries
- \* Q167038 RAS Clients Run Winsock and RPC Applications Slowly
- \* Q167044 Request From Perfmon Counter Can Cause Excessive Page Faults
- \* Q167110 NT 4.0 RAS client slows over time due to lack of resources
- \* Q167129 Stop 0x7A or System Lockup in NTBACKUP With MINIQC
- \* Q167130 Fatal System Error in NDIS.SYS Allocating Map Registers
- \* Q167362 STOP 0x00000050 in SRV.SYS When Shutting Down Computer Service Pack 2
- \* Q108261: Windows NT Hangs on Shutdown with Certain PCMCIA Devices
- \* Q140059: Stop 0xA in Afd When Browsing IIS
- \* Q140065: Multi-Processor Systems Randomly Restart or Stop Responding
- \* Q141375: Winstone 97 May Fail on Windows NT 4.0
- \* Q142634: Multiple Processes Are Able to Open the Same Winsock Port
- \* Q142641: Internet Server Unavailable Because of Malicious SYN Attacks
- \* Q142648: STOP 0x00000024 in Ntfs.sys
- \* Q142656: Internet Explorer 3.0 on RISC Computer Cannot Connect to Host
- \* Q142671: Backup Fails on Certain Directories Due to Lack of Permissions
- \* Q142675: CSNW Sends Packets Greater Than Negotiated Maximum Packet Size
- \* Q142686: First Line of Print Job Lost When Printing Using Lpdsvc
- \* Q142687: Windows NT 4.0 Not Able to Read Some Compact Discs
- \* Q142847: Bugcheck 0x1e Caused by Isotp.sys Driver
- \* Q142872: Length of PDC Name May Affect Performance on a Domain
- \* Q142903: Windows NT Ndis.sys and Netflx3.sys Performance Improvement
- \* Q146336: Joystick in Windows NT 4.0 Does Not Work Properly
- \* Q147363: AlphaServer Hangs on Install of Windows NT Version 4.0
- \* Q147497: Matrox Video Driver May Fail on Alpha-based Computers
- \* Q147552: Backup Always Reports Time as PM
- \* Q148378: Setup of RAS with Multiple Modems Gives Slow Performance
- \* Q148525: Removable Media Does Not Eject if Formatted in NTFS
- \* Q148602: Running SNA Server 2.11 on the Windows NT 4.0
- \* Q150815: Windows NT May Fail to Boot on Toshiba Portable Computers
- \* Q153665: SPX Data Stream Type Header May Reset Unexpectedly
- \* Q154556: Delegation Requires a Stop and Restart of the DNS Server Service
- \* Q154620: Windows NT 4.0 DNS Server Loses the Forwarders Settings
- \* Q154784: Windows NT Operating System SNMP OID Incorrect
- \* Q155883: NT 4.0 Breaks SNA Server 2.x Server Communication Over IP
- \* Q156091: Access Violation with Long NDS Context in CSNW/GSNW
- \* Q156095: Replace Command with Space Character in the Path Does Not Work
- \* Q156276: Cmd.exe Does Not Support UNC Names as the Current Directory
- \* Q156324: Device Failure Message with Microchannel Network Adapter
- \* Q156520: Logon Validation Fails Using Domain Name Server (DNS)
- \* Q156578: Cannot Cancel Print Job on Windows NT 3.51 Shared Printer
- \* Q156735: WOW Applications Stack Fault When Launched by a Service
- \* Q156746: Print Jobs Are Deleted When Printer Is Resumed After Restart
- \* Q156750: AddGroupNameResponse Frame from WinNT May Cause WFWG to Hang
- \* Q156884: Problems Saving Event Viewer Log from Windows NT 4.0 to 3.51

# UNCLASSIFIED

- \* Q156958: Serial Service Won't Stop with Serial Printer Installed
- \* Q157279: Nwrdr.sys Fails Reading File with Execute Only Attribute
- \* Q157289: Memory Leak Using RegConnectRegistry API
- \* Q157494: PPC 4.0 Cirrus Driver Fails to Redraw & Fill Objects Correctly
- \* Q157621: Personal Groups Not Visible If %Systemroot% Is Read-Only
- \* Q157673: Policy Not Updated on Workstation
- \* Q158142: WM\_DDE\_EXECUTE API Causes a Memory Leak in the WOW Subsystem
- \* Q158387: RAS Server Cannot Use DHCP to Assign Addresses w/ PPTP Filtering
- \* Q158587: 16-Bit Named Pipe File Open Leads to WOW Access Violation
- \* Q158682: Shortcuts Created Under NT 4.0 Resolve to UNC Paths
- \* Q158707: DDE Destroy Window Code May Stop 0x0000001e in Windows NT 4.0
- \* Q158796: Macintosh Clients Connected to WinNT Server Appear to Hang
- \* Q158981: IBM Thinkpads 760ED and 760ELD May Hang During Shutdown
- \* Q159053: NTFS Stream Limitation in Windows NT 4.0
- \* Q159066: A Client Crash May Prevent an NTFS Volume Dismount
- \* Q159071: NTFS Does Not Prevent a File Deletion During Rename
- \* Q159072: An Account That Still Has System Access May Be Deleted
- \* Q159073: Screen Corruption on Dell Laptops Using Cirrus Video
- \* Q159075: Compression Is Not Supported on Quantum 4000DLT
- \* Q159076: Windows NT 4.0 May Hang or Crash in Win32k.sys During Setup.
- \* Q159085: Windows NT Kernel Crashes While Processing WM\_NCCREATE
- \* Q159090: Delphi 2.00 and 2.01 Users Encounter Error 998
- \* Q159091: German Time Zone Results in Incorrect Log Times
- \* Q159092: Mouse Buttons Not Swapped on German Windows NT 4.0
- \* Q159093: Windows NT Muldiv() Function Returns Incorrect Value
- \* Q159095: STOP 0x0000001E in Win32k.sys When Exiting Applications
- \* Q159098: WinNT 4.0 Resource Kit Utility "Remote Console" Client Fails
- \* Q159105: Cannot Open Truncated File Names from Compact Discs
- \* Q159107: Access Violaion in AddAtom Inside Kernel32.dll
- \* Q159108: SMP Full Duplex Adapter Configuration May Cause a Blue Screen
- \* Q159109: ExitWindowsEx Does Not Work With NEC Power Switch Service
- \* Q159110: CDFS Does Not Complete IRPs Correctly
- \* Q159111: Multiprocessor Computer Hangs Under Stress Using Halsp.dll
- \* Q159119: NTFS Generates Cross-Linked Files
- \* Q159127: Bugcheck in Windows NT While Running POSIX Applications
- \* Q159129: OpenGL Access Violation with Invalid OpenGL Context
- \* Q159137: Moving Files Can Corrupt NTFS Partition
- \* Q159141: CDFS Incorrectly Creates Short File Names for Some Files
- \* Q159144: Dongle May Not Function Under Windows NT 4.0
- \* Q159203: Unattended Install Prompts for New IP if Zero Is in Address
- \* Q159204: IoCompletionPort Causes Blue Screen Error
- \* Q159205: SFM File Type and Creator Properties Invalid
- \* Q159206: Reactivation of Paused Print Queues Deletes Print Jobs
- \* Q159309: Windows NT 4.0 RAS Not Releasing Static IP Addresses
- \* Q159352: RPC over NetBIOS Programs Can't Call from Server to RAS Client
- \* Q159447: Applications Testing for Directory Existence Fail
- \* Q159449: DNS Server Glue Data Is Deleted
- \* Q159450: Second Recursive Query Sent from DNS Server Is Broken
- \* Q159594: Missing Eastern Europe FontSubstitutes in Registry
- \* Q159910: Memory Corruption on a Windows NT Alpha Platform
- \* Q159970: Slow List of Folders and Files with CSNW
- \* Q159971: SetTimer() API Causes Memory Leak in the WOW Subsystem
- \* Q159972: WinNT 4.0 May Not Return Valid Response for SMB Search Command

# UNCLASSIFIED

- \* Q160015: 2D Vector Performance on WinNT 4.0 Slower Than on 3.51
- \* Q160055: Warning Event ID 4010 Generated on Windows NT LPD Server
- \* Q160189: CSNW Cannot See More Than 32 Volumes Per Server
- \* Q160190: RasSetEntryProperties Does Not Save a Full Path Script Name
- \* Q160354: Mouse and Keyboard Can Disappear when Replacing Drivers
- \* Q160370: Stop Screen 0x00000050 Caused by Fs\_rec.sys
- \* Q160372: Intermittent File Corruption when Compiling on NTFS Partition
- \* Q160373: Adaptec Aic78xx Does Not Issue Multiple Tagged Commands
- \* Q160377: File Size Data Does Not Remain Consistent After Defrag on NTFS
- \* Q160392: Systems with 4 GB or More of RAM Cannot Boot Windows NT 4.0
- \* Q160398: Cannot Read Files Greater than 4 GB
- \* Q160404: Madge EISA Stops Responding on Alpha in Windows NT 4.0
- \* Q160405: Video Memory Not Correctly Detected on Dell Latitude Laptops
- \* Q160420: Changing Colors on Cirrus Logic Cards to 65k Can Cause Stop
- \* Q160459: DNS Delegations May Fail
- \* Q160470: Stop 0x0000000a IPX Sends Browser an Incomplete Datagram
- \* Q160493: NWLNKRIP Data Structures Corruption when Using a Demand Dial NIC
- \* Q160494: DNS Zone Transfer Fails After WINS Record Added
- \* Q160497: Cache File Entries Disappear
- \* Q160508: Unnecessary DNS Zone Transfers
- \* Q160518: Zone Files in Multiples of 4 KB May Cause Access Violation
- \* Q160583: Windows NT 4.0 with More Than 4 Processors May Stall & Reboot
- \* Q160601: Bad Parameters Sent to Win32k.sys May Cause Stop Message
- \* Q160603: No Output from DBMON Using OutputDebugString While Debugging
- \* Q160604: Access Violation in security!SspQueryContextAttributesW
- \* Q160606: Performance Enhancements for SQL Server Under Windows NT
- \* Q160610: READ\_REGISTER\_ULONG Doesn't Preserve ULONG Semantics on Alpha
- \* Q160649: STOP 0x0000000A in Ntoskrnl.exe at Logon to Windows NT 4.0
- \* Q160650: Blue Screen When Closing Kernel Mode Handles from User Mode
- \* Q160651: OpenGL May Cause an Exception 0xc0000090
- \* Q160653: NTFS Fails Assertion Under High Stress During Transfer
- \* Q160657: 16-bit Version of Visual Basic 4 May Hang Windows NT 4.0
- \* Q160658: Stop C0000021A Using MoveFileEx MOVEFILE\_DELAY\_UNTIL\_REBOOT
- \* Q160670: FPSCR is Not Being Saved Across Thread Context Switches
- \* Q160671: Stop 0x0000007F May Occur on Compaq SystemPro
- \* Q160678: Possible Access Violation in Win32k.sys Under High Stress
- \* Q160702: Event 2006 Errors in Xcopy from WinNT 4.0 to OS/2 3.0 Client
- \* Q160732: FIX: SQL Server 6.5 Service Pack 2 Fixlist (Part 2 of 2)
- \* Q160791: Excel Charts Lose Color When Pasted into Word
- \* Q160840: Sharing Violation When Accessing User Profiles
- \* Q160894: Incoming Fax Jobs Do Not Appear in Print Queue
- \* Q160964: 0x0000001e When Printing Certain Documents from Windows NT 4.0
- \* Q161201: NTBackup.exe from WinNT 3.51 SP5 Causes Verify Errors
- \* Q161802: Stop 0x0000000A During Create File SMB
- \* Q161990: How to Enable Strong Password Functionality in Windows NT
- \* Q162157: Cyberbit Unicode Font Does Not Return Correct Charset
- \* Q163055: DHCP Client May fail with NT 4.0 SP2 Multinetted DHCP Server
- \* Q163736: Access Violation in DNS Manager when deleting cached domain
- \* Q163772: Nested "for" Loops Using the '~' Operators Does not Work
- \* Q163773: Brief 3.0 in NTVDM Consumes 100% Processor
- \* Q163837: SNMP query to Windows NT returns same value for NTS and NTW Service Pack 1
- \* Q78303: Intermittent File Corruption Problem

UNCLASSIFIED

## UNCLASSIFIED

- \* Q142653: STOP Message Occurs Calling GetThreadContext/SetThreadContext
- \* Q142654: Winsock Memory Access Violation in Ws2help.dll Or Msafd.dll
- \* Q142655: Stop Message Appears After Deleting ProductOption Registry Key
- \* Q142656: Internet Explorer 3.0 on RISC Computer Cannot Connect to Host
- \* Q142657: Data Corruption on Windows NT 4.0
- \* Q142658: Internet Information Server Runs Out of Memory
- \* Q149903: File Manager Performs a Move Instead of a Copy
- \* Q156832: STOP Message when IBM Warp Client Connects to Windows NT 4.0

## (U) Windows NT 4.0 Post Service Pack 4 Hotfix Information

(U) Below is a list of post Service Pack 4 hotfixes, along with the software versions containing or affected by the problem, the date of the hotfix, where to download the fix, the size of the compressed executable, and a Microsoft Knowledge Base article number to find out more information about the hotfix. The Microsoft Knowledge Base is located at <http://www.microsoft.com/kb/default.asp>. The ftp web sites mentioned may also be accessed by executing `ftp microsoft.com` and then changing directory to the `/bussys/winnt-public/fixes/usa/nt40/hotfixes-postsp4`.

(U) NOTE: Several hotfixes supercede older fixes. When this occurs, the superceded fixes are mentioned within the newer fix, but do not have their own entry in the list below.

### Master Hotfix.inf

; hotfix.inf

; This is a sample hotfix.inf file for group installation of  
; security-related post-SP4 hotfixes in conjunction with  
; Service Pack 4. The hotfixes included are: nprpc-fix,  
; tcpip-fix, and sms-fix.

; Last modified 12/22/98

[Version]

Signature="\$Windows NT\$"

NtBuildToUpdate=1381

NtMajorVersionToUpdate=4

NtMinorVersionToUpdate=0

NtServicePackVersion=1024

NtMinimumServicePackVersion=1024

HotfixNumber=%HOTFIX\_NUMBER%

LanguageType=%LangTypeValue%

InstallPlatform=0

RequiredFreeSpaceNoUninstall=5

RequiredFreeSpaceWithUninstall=5

[ProductInstall.ReplaceFilesIfExist]

CopyFiles=System32.files

CopyFiles=SystemRoot.files

CopyFiles=Inf.files

# UNCLASSIFIED

CopyFiles=Spldr.files  
CopyFiles=Fonts.files

[ProductInstall.DontDelayUntilReboot]

;  
; These files must be replaced before rebooting, not delayed-until-reboot,  
; because they are loaded before the delay-until-reboot code is executed.  
;

CopyFiles=MustReplace.System32.files  
CopyFiles=Drivers.files  
CopyFiles=Osldr.files

[ProductInstall.CopyFilesAlways]

CopyFiles=CopyAlways.System32.files  
CopyFiles=CopyAlways.Drivers.files  
CopyFiles=CopyAlways.Inf.files

[ProductInstall.ServerFiles]

CopyFiles=Server.Inf.files

[ProductInstall.WorkstationFiles]

CopyFiles=Workstation.Inf.files  
DelReg=Product.Del.Reg.Workstation

[ProductInstall.UniprocessorFiles]

CopyFiles=Uniprocessor.Kernel.files

[ProductInstall.MultiprocessorFiles]

CopyFiles=Multiprocessor.Kernel.files

[ProductInstall.GlobalRegistryChanges]

AddReg=Product.Add.Reg, Product.RunOnce

[ProductInstall.GlobalRegistryChanges.x86]

AddReg=Product.Add.Reg.x86

[ProductInstall.GlobalRegistryChanges.Alpha]

AddReg=Product.Add.Reg.Alpha

[ProductInstall.GlobalRegistryChanges.PPC]

AddReg=Product.Add.Reg.PPC

[IBM-6070.Section]

AddReg=IBM-6070.AddReg

# UNCLASSIFIED

## [IISSection]

CopyFiles=IIS.files  
CopyFiles=IISAdmin.files  
AddReg=IIS.AddReg

## [IISSectionServer]

CopyFiles=Server.IIS.Inf.files  
AddReg=Server.IIS.AddReg

## [IISSectionWorkstation]

CopyFiles=Workstation.IIS.Inf.files  
AddReg=Workstation.IIS.AddReg

## [FPNWSection]

CopyFiles=FPNW.files

## [HTRSection]

CopyFiles=HTR.files

## [IESection]

CopyFiles=IE.files

## [HyperSection]

CopyFiles=Hyper.files

## [EudcSection]

CopyFiles=Eudc.files

## [ClusterSection]

CopyFiles=Cluster.files

## [Save.Reg.For.Uninstall]

## [Save.Reg.For.Uninstall]

HKLM,SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\%SERVICE\_PACK%\Hotfix\%HOTFIX\_NUMBER%

## [Product.Add.Reg]

HKLM,SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\%SERVICE\_PACK%\Hotfix\%HOTFIX\_NUMBER%,"Installed",0x10001,1  
HKLM,SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\%SERVICE\_PACK%\Hotfix\%HOTFIX\_NUMBER%,"Comments",0,%COMMENT  
%

# UNCLASSIFIED

```
HKLM,SOFTWARE\Microsoft\Windows
NT\CurrentVersion\%SERVICE_PACK%\Hotfix\%HOTFIX_NUMBER%,"Backup Dir",0,""
HKLM,SOFTWARE\Microsoft\Windows
NT\CurrentVersion\%SERVICE_PACK%\Hotfix\%HOTFIX_NUMBER%,"Fix
Description",0,%COMMENT%
HKLM,SOFTWARE\Microsoft\Windows
NT\CurrentVersion\%SERVICE_PACK%\Hotfix\%HOTFIX_NUMBER%,"Installed By",0,""
HKLM,SOFTWARE\Microsoft\Windows
NT\CurrentVersion\%SERVICE_PACK%\Hotfix\%HOTFIX_NUMBER%,"Installed On",0,""
HKLM,SOFTWARE\Microsoft\Windows
NT\CurrentVersion\%SERVICE_PACK%\Hotfix\%HOTFIX_NUMBER%,"Valid",0x10001,1
HKLM,SOFTWARE\Microsoft\Windows
NT\CurrentVersion\%SERVICE_PACK%\Hotfix\%HOTFIX_NUMBER%\File 1,"Flags",0,""
HKLM,SOFTWARE\Microsoft\Windows
NT\CurrentVersion\%SERVICE_PACK%\Hotfix\%HOTFIX_NUMBER%\File 1,"New File",0,""
HKLM,SOFTWARE\Microsoft\Windows
NT\CurrentVersion\%SERVICE_PACK%\Hotfix\%HOTFIX_NUMBER%\File 1,"New Link Date",0,""
HKLM,SOFTWARE\Microsoft\Windows
NT\CurrentVersion\%SERVICE_PACK%\Hotfix\%HOTFIX_NUMBER%\File 1,"Old Link Date",0,""
```

[Product.RunOnce]

[DestinationDirs]

```
SystemRoot.files=10 ; %windir% (replace if exist)

System32.files=11 ; %windir%\system32 (replace if exist)
CopyAlways.System32.files=11 ; %windir%\system32 (copy even if don't exist)
MustReplace.System32.files=11 ; %windir%\system32 (don't delay until reboot)
CheckSecurity.System32.files=11 ; %windir%\system32 (warn if 40-bit replacing 128-bit)

Drivers.files=12 ; %windir%\system32\drivers (don't delay until reboot)
CopyAlways.Drivers.files=12 ; %windir%\system32\drivers (copy even if don't exist)
CheckSecurity.Drivers.files=12 ; %windir%\system32 (warn if 40-bit replacing 128-bit)

Uniprocessor.Kernel.files=11 ; %windir%\system32 (don't delay until reboot)
Multiprocessor.Kernel.files=11 ; %windir%\system32 (don't delay until reboot)

Hal.files.x86=11 ; %windir%\system32 (don't delay until reboot)
Hal.files.Alpha=54 ; osloader.exe location (don't delay until reboot)
Hal.files.PPC=54 ; osloader.exe location (don't delay until reboot)

Oslldr.files=54 ; path to ntldr or osloader.exe (don't delay until reboot)

Inf.files=17 ; %windir%\inf (replace if exist)
CopyAlways.Inf.files=17 ; %windir%\inf (copy even if don't exist)
Server.Inf.Files=11 ; %windir%\system32 (replace if exist)
Workstation.Inf.Files=11 ; %windir%\system32 (replace if exist)

Fonts.files=20 ; %windir%\fonts (replace if exist)
Spldrv.files=52,2 ; %windir%\system32\spool\drivers\<platform>\2

IIS.files=65601 ; destination determined at runtime
IISAdmin.files=65601,iisadmin ; destination determined at runtime
FPNW.files=65602 ; destination determined at runtime
HTR.files=65603 ; destination determined at runtime
```

# UNCLASSIFIED

IE.files=65604 ; destination determined at runtime  
Hyper.files=65605 ; destination determined at runtime  
Eudc.files=65606 ; destination determined at runtime  
Cluster.files=65607 ; destination determined at runtime  
Server.IIS.Inf.Files=65601 ; destination determined at runtime  
Workstation.IIS.Inf.Files=65601 ; destination determined at runtime

[MustReplace.System32.files]

; nprpc-fix  
RPCLTS1.DLL

; sms-fix  
ADVAPI32.DLL  
PERFCTRS.DLL  
SNMP.EXE  
TAPIPERF.DLL  
WINLOGON.EXE

[CopyAlways.System32.files]

[CopyAlways.Drivers.files]

[CopyAlways.Inf.files]

[SystemRoot.files]

[System32.files]

[Drivers.files]

; tcpip-fix  
TCPIP.SYS

[Osldr.files]

[Inf.files]

[Spldrv.files]

[Fonts.files]

[Uniprocessor.Kernel.files]

[Multiprocessor.Kernel.files]

[IIS.files]

[FPNW.files]

[HTR.files]

[IE.files]

[Hyper.files]

# UNCLASSIFIED

[Eudc.files]

[Cluster.files]

[IISAdmin.files]

[Server.IIS.Inf.Files]

[Server.Inf.files]

[Workstation.IIS.Inf.Files]

[Workstation.Inf.files]

[Check.For.128.Security]

; Although this section is structured as an "Install" section with  
; "CopyFiles" sections, it only causes these files to be checked, not  
; copied. Any files in these sections must also be specified in the  
; appropriate "CopyFiles" sections of a real "Install" section to  
; cause them to be copied.

CopyFiles = CheckSecurity.System32.files

CopyFiles = CheckSecurity.Drivers.files

[CheckSecurity.System32.files]

[CheckSecurity.Drivers.files]

[SourceDisksNames]

1=%ServicePackSourceFiles%

[SourceDisksFiles]

; nprpc-fix  
RPCLTS1.DLL = 1

; tcpip-fix  
TCPIP.SYS = 1

; sms-fix  
ADVAPI32.DLL = 1  
PERFCTRS.DLL = 1  
SNMP.EXE = 1  
TAPIPERF.DLL = 1  
WINLOGON.EXE = 1

[SourceDisksFiles.x86]

[SourceDisksFiles.Alpha]

[Strings]

LangTypeValue=9  
ServicePackSourceFiles="Windows NT 4.0 Hotfix Source Files"

# UNCLASSIFIED

SERVICE\_PACK="SP4"  
HOTFIX\_NUMBER="SP4 Hotfix Group"  
COMMENT="The following post SP4 hotfixes have been applied: nprpc-fix (fix for named pipe RPC denial of service; tcpip-fix (TCP/IP crashing fix for 3Com drivers); sms-fix (fix for memory leaks in TAPI, SNMP, and PERFCTRS)"

**RPC-Hotfix****Knowledge Base:**Q195733**Title:**Denial of Service in Applications Using Named Pipes over RPC**Applies to:**

- Microsoft Windows NT Workstation version 4.0
- Microsoft Windows NT Server version 4.0
- Microsoft Windows NT Server, Enterprise Edition version 4.0
- Microsoft Windows NT Server 4.0, Terminal Server Edition

**Download from:** <ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP4/nprpc-fix/>**File Name:** Nprpcfxi.exe (x86) and Nprpcfxa.exe (Alpha):**File Attributes:**

Date	Time	Size	File name	Platform
11/12/98	03:38p	12,048	Rpclts1.dll	(x86)
11/12/98	03:37p	23,312	Rpclts1.dll	(Alpha)

**Symptoms:**

Windows NT computer responsiveness appears sluggish, and network clients may report a gradual decrease in system performance because of a Windows NT system process consuming 100 percent of CPU time. In addition, system memory usage may continually increase (potentially indicating a memory leak of system resources) up to the limit of available memory. The computer may stop responding (hang).

**Cause:**

This problem is caused by a malicious attack on the remote procedure call (RPC) components in Windows NT using named pipes transport. Specific instances of this denial of service attack may be targeted at either the Spoolss.exe file or Lsass.exe file. There are different variations of the attack and each may create multiple named pipe connections to a Windows NT system and send random data. The RPC service then attempts to send a response and close each connection. The RPC service then cycles into a 100 percent CPU usage loop closing the invalid connections.

**Resolution:**

Windows NT Server and Workstation  
Windows NT Server, Enterprise Edition

Microsoft has confirmed this problem could result in some degree of security vulnerability in Windows NT version 4.0. A fully supported fix is now available, but it has not been fully regression tested and should only be applied to systems determined to be at risk of attack. Please evaluate your system's physical accessibility, network and Internet connectivity, and other factors to determine the degree of risk to your system. If your system is sufficiently at risk, Microsoft recommends you apply this fix. Otherwise, wait for the next Windows NT service pack, which will contain this fix. To resolve this problem immediately, download the fix as described above.

Windows NT Server 4.0, Terminal Server Edition

Microsoft has confirmed this problem could result in some degree of security vulnerability in Windows NT version 4.0, Terminal Server Edition. A fully supported fix will be available soon.

**Status**

Windows NT Server and Workstation  
Windows NT Server, Enterprise Edition

Microsoft has confirmed this problem could result in some degree of security vulnerability in Windows NT version 4.0, and Windows NT Server 4.0, Terminal Server Edition

**More Information:**

Using Windows NT Performance Monitor, you observe that, over time, the computer's CPU usage increases to 100 percent and remains there.

THE INFORMATION PROVIDED IN THE MICROSOFT KNOWLEDGE BASE IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. MICROSOFT DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO

## UNCLASSIFIED

EVENT SHALL MICROSOFT CORPORATION OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER INCLUDING DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF MICROSOFT CORPORATION OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES SO THE FOREGOING LIMITATION MAY NOT APPLY.

**TCP-Hotfix****Knowledge Base:** Q195725**Title:** Intermediate Network Driver Causes STOP 0x0000001E on MP PC**Applies to:**

- Microsoft Windows NT Workstation version 4.0
- Microsoft Windows NT Server version 4.0

**Download from:** <ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP4/Tcpip-fix/>**File Name:** Tcpipfxi.exe (x86) and Tcpipfxa.exe (Alpha):**File Attributes;**

Date	Time	Size	File Name	Platform
11/11/98	12:13p	147,664	Tcpip.sys	(x86)
11/11/98	12:13p	268,880	Tcpip.sys	(Alpha)

**Symptoms:**

After you install an intermediate network driver, such as the Dynamic Access Intermediate driver from 3COM Corporation, the Windows NT computer may display a blue screen error message in Tcpip.sys with a STOP 0x0000000E. The second dword of the stop code will be 0xC0000005. This has only been observed on multiprocessor computers. An intermediate driver is a network driver that is layered between a transport driver and a miniport driver to provide added functionality.

**Cause:**

The Tcpip.sys driver does not properly initialize on multiprocessor computers.

**Resolution:**

A supported fix that corrects this problem is now available from Microsoft, but has not been fully regression tested and should be applied only to systems experiencing this specific problem. If you are not severely affected by this specific problem, Microsoft recommends that you wait for the next Windows NT service pack that contains this fix. To resolve this problem immediately, download the fix as described above.

**Status**

Microsoft has confirmed this to be a problem in Windows NT version 4.0.

THE INFORMATION PROVIDED IN THE MICROSOFT KNOWLEDGE BASE IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. MICROSOFT DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL MICROSOFT CORPORATION OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER INCLUDING DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF MICROSOFT CORPORATION OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES SO THE FOREGOING LIMITATION MAY NOT APPLY.

**Sms-fix**

**Knowledge Base:** Q196270

**Title:** SNMP Agent Leaks Memory When Queried

**Applies to;**

- Microsoft Windows NT Workstation version 4.0
- Microsoft Windows NT Server version 4.0
- Microsoft Windows NT Server, Enterprise Edition version 4.0

**Download from:** <ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP4/Sms-fix/>

**File Name:** Smsfixi.exe (x86) and Smsfixa.exe (Alpha):

**File Attributes:**

This hotfix was updated on December 17, 1998.

**Symptoms**

The SNMPtest utility exhibits substantial memory leakage when it is used to stress the SNMP agent.

**Cause**

This problem occurs because, while processing messages, a buffer was used that was never freed.

**Resolution:**

A supported fix that corrects this problem is now available from Microsoft, but has not been fully regression tested and should be applied only to systems experiencing this specific problem. If you are not severely affected by this specific problem, Microsoft recommends that you wait for the next Windows NT service pack that contains this fix. To resolve this problem immediately, download the fix as described above.

**Status**

Microsoft has confirmed this to be a problem in Windows NT version 4.0.

THE INFORMATION PROVIDED IN THE MICROSOFT KNOWLEDGE BASE IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. MICROSOFT DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL MICROSOFT CORPORATION OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER INCLUDING DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF MICROSOFT CORPORATION OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES SO THE FOREGOING LIMITATION MAY NOT APPLY.

**Clik-fix****Knowledge Base:** Q195540**Title:** Windows NT 4.0 Does Not Recognize ATAPI Iomega Clik 40! Drive**Applies to:**

- Microsoft Windows NT Server version 4.0
- Microsoft Windows NT Workstation version 4.0
- Microsoft Windows NT Server, Enterprise Edition version 4.0

**Download from:** <ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP4/Clik-fix/>**File Name:** Clikfixi.exe (x86) and Clikfixa.exe (Alpha):**File Attributes:**

Date	Time	Size	File Name	Platform
11/06/98	03:47p	13,744	Class2.sys	(x86)
11/06/98	03:46p	23,440	Class2.sys	(Alpha)

**Symptoms:**

Windows NT 4.0 cannot access the ATAPI version of the Iomega Clik 40! drive.

**Cause:**

Windows NT identifies the ATAPI version of the Iomega Clik 40! drive as a floppy disk drive and assigns it the first available floppy disk drive letter (usually drive B).

**Resolution**

A supported fix that corrects this problem is now available from Microsoft, but has not been fully regression tested and should be applied only to systems experiencing this specific problem. If you are not severely affected by this specific problem, Microsoft recommends that you wait for the next Windows NT service pack that contains this fix. To resolve this problem immediately, download the fix as described above.

**Status:**

Microsoft has confirmed this to be a problem in Windows NT version 4.0.

THE INFORMATION PROVIDED IN THE MICROSOFT KNOWLEDGE BASE IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. MICROSOFT DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL MICROSOFT CORPORATION OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER INCLUDING DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF MICROSOFT CORPORATION OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES SO THE FOREGOING LIMITATION MAY NOT APPLY.

**(U) PDC.inf**

## [System Access]

MinimumPasswordAge = 1  
MaximumPasswordAge = 90  
MinimumPasswordLength = 12  
PasswordComplexity = 1  
PasswordHistorySize = 24  
LockoutBadCount = 3  
ResetLockoutCount = 15  
LockoutDuration = 15  
RequireLogonToChangePassword = 1  
ForceLogoffWhenHourExpire = 1

## [System Log]

MaximumLogSize = 4194240  
AuditLogRetentionPeriod = 2  
RestrictGuestAccess = 1

## [Security Log]

MaximumLogSize = 4194240  
AuditLogRetentionPeriod = 2  
RestrictGuestAccess = 1

## [Application Log]

MaximumLogSize = 4194240  
AuditLogRetentionPeriod = 2  
RestrictGuestAccess = 1

## [Event Audit]

AuditSystemEvents = 3  
AuditLogonEvents = 3  
AuditObjectAccess = 2  
AuditPrivilegeUse = 2  
AuditPolicyChange = 3  
AuditAccountManage = 3  
AuditProcessTracking = 0  
CrashOnAuditFull = 1

## [Version]

signature="\$CHICAGO\$"

## [Group Membership]

## [Service General Setting]

Schedule,4,"D:(A;0x000200ad;;;DA)(A;0x000201fd;;;SY)S:(SA;FA;0x000f01ff;;;WD)"

# UNCLASSIFIED

## [Registry Values]

MACHINE\System\CurrentControlSet\Control\Lsa\FullPrivilegeAuditing=3,30  
MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous=4,1  
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon>PasswordExpiryWarning=15  
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateCDRoms=1,1  
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateFloppies=1,1  
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount=1,0  
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\DontDisplayLastUserName=1,1  
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\LegalNoticeCaption=1,.... <<<<  
Message Title for Users Logging on >>>> ....  
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\LegalNoticeText=1,.... <<<  
Message Text for Users Logging on >>> ....  
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ShutdownWithoutLogon=1,0  
MACHINE\System\CurrentControlSet\Control\Lsa\CrashOnAuditFail=4,1  
MACHINE\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel=4,1  
MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print  
Services\AddPrintDrivers=4,1  
MACHINE\System\CurrentControlSet\Control\Session Manager\Memory  
Management\ClearPageFileAtShutdown=4,1  
MACHINE\System\CurrentControlSet\Control\Session Manager\ProtectionMode=4,1  
MACHINE\System\CurrentControlSet\Services\Rdr\Parameters\EnablePlainTextPassword=4,0

## [Registry Keys]

"MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg",2,"D:P(A;CI;0x000f003f;;DA)(A;CI;0x000f003f;;;SY)"  
"MACHINE\SOFTWARE\Windows 3.1 Migration  
Status",2,"D:P(A;CI;0x000f003f;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;CO)(A;CI;0x000f003f;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx",2,"D:P(A;CI;0x000f003f;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time  
Zones",2,"D:P(A;CI;0x000f003f;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run",2,"D:P(A;CI;0x000f003f;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;SY)"  
"MACHINE\SOFTWARE\Microsoft\OS/2 Subsystem for  
NT",2,"D:P(A;CI;0x000f003f;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;CO)(A;CI;0x000f003f;;SY)"  
"MACHINE\HARDWARE",2,"D:P(A;CI;0x000f003f;;DA)(A;CI;0x0002001f;;;AU)(A;CI;0x000f003f;;CO)(A;CI;0x000f003f;;;SY)"  
"USERS\DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies",2,"D:P(A;CI;0x000f003f;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;CO)(A;CI;0x000f003f;;SY)"  
"USERS\DEFAULT\SOFTWARE\Microsoft\NetDDE",2,"D:P(A;CI;0x10000000;;DA)(A;CI;0x10000000;;SY)"  
"USERS\DEFAULT",2,"D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;DA)(A;CI;0x10000000;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\Winlogon",2,"D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;DA)(A;CI;0x10000000;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\Perflib",2,"D:P(A;CI;0x000f003f;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\IniFileMapping",2,"D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;DA)(A;CI;0x10000000;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution  
Options",2,"D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;DA)(A;CI;0x10000000;;SY)"

# UNCLASSIFIED

"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontMapper",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Font Drivers",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Windows NT",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce",2,"D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Windows",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x0002001f;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Secure",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Rpc",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Ole",2,"D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;CO)(A;CI;0x10000000;;;SY)"

"MACHINE\SOFTWARE\Microsoft\NetDDE",2,"D:P(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Cryptography",2,"D:P(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)(A;CI;0x80000000;;;AU)"

"MACHINE\SOFTWARE\Classes",1,""

"CLASSES\_ROOT\helpfile",2,"D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"

"CLASSES\_ROOT",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x0002001f;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"

"MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Shares",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"

"MACHINE\SYSTEM\CurrentControlSet\Services\Schedule",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"

"MACHINE\SYSTEM\CurrentControlSet\Services\UPS",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"

"USERS\DEFAULT\SOFTWARE\Microsoft\Protected Storage System Provider",1,""

"MACHINE\SOFTWARE\Secure",2,"D:P(A;CI;0x10000000;;;CO)(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"

"MACHINE\SOFTWARE\Program Groups",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\009",1,""

"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Compatibility",2,"D:P(A;CI;0xc0000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;CO)(A;CI;0x10000000;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Protected Storage System Provider",1,""

"MACHINE\SOFTWARE",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x0003001f;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"

"CLASSES\_ROOT\hip",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Shell Extensions",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"

[File Security]

UNCLASSIFIED

"%SystemRoot%\mapiuid.ini",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001301bf;;;AU)(A;C:IOI;0x001f01ff;;;CO)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemRoot%\drwtsn32.log",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001301bf;;;AU)(A;C:IOI;0x001f01ff;;;CO)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemRoot%\nsreg.dat",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001301bf;;;AU)(A;C:IOI;0x001f01ff;;;CO)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDirectory%\spool\Printers",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001301bf;;;AU)(A;C:IOI;0x001f01ff;;;CO)(A;C:IOI;0x001301bf;;;RP)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemRoot%",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001200a9;;;AU)(A;C:IOI;0x001f01ff;;;CO)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDirectory%",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001200a9;;;AU)(A;C:IOI;0x001f01ff;;;CO)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemRoot%\\$NtServicePackUninstall\$",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDrive%",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001201bf;;;AU)(A;C:IOI;0x001f01ff;;;CO)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDirectory%\rep\export",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001200a9;;;AU)(A;C:IOI;0x001f01ff;;;CO)(A;C:IOI;0x001200a9;;;RP)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDirectory%\rep\import",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001200a9;;;AU)(A;C:IOI;0x001f01ff;;;CO)(A;C:IOI;0x001301bf;;;RP)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDirectory%\config",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemRoot%\repair",2,"D:P(A;C:IOI;0x10000000;;;DA)(A;C:IOI;0x10000000;;;SY)"  
"%SystemDrive%\Program Files",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001201bf;;;AU)(A;C:IOI;0x001f01ff;;;CO)(A;C:IOI;0x001f01ff;;;SY)"  
"c:\config.sys",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001200a9;;;AU)(A;C:IOI;0x001f01ff;;;SY)"  
"c:\autoexec.bat",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001200a9;;;AU)(A;C:IOI;0x001f01ff;;;SY)"  
"c:\ntldr",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"  
"c:\ntdetect.com",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"  
"c:\boot.ini",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDrive%\Users",1,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001201bf;;;AU)(A;C:IOI;0x001f01ff;;;CO)(A;C:IOI;0x001f01ff;;;S-0x1-0x000000000005-0x15-0x3b1e46f5-0x69bf70fb-0x253b7c20-0x200)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDrive%\Win32app",1,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001201bf;;;AU)(A;C:IOI;0x001f01ff;;;CO)(A;C:IOI;0x001f01ff;;;S-0x1-0x000000000005-0x15-0x3b1e46f5-0x69bf70fb-0x253b7c20-0x200)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemRoot%\Profiles",1,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001201bf;;;AU)(A;C:IOI;0x001f01ff;;;CO)(A;C:IOI;0x001f01ff;;;S-0x1-0x000000000005-0x15-0x3b1e46f5-0x69bf70fb-0x253b7c20-0x200)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDrive%\lo.sys",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001200a9;;;AU)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDrive%\ntldr",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDrive%\Config.sys",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001200a9;;;AU)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDrive%\Msdos.sys",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001200a9;;;AU)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDrive%\Ntdetect.com",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDrive%\boot.ini",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDrive%\Autoexec.bat",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001200a9;;;AU)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDrive%\NTReskit",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001200a9;;;AU)(A;C:IOI;0x001f01ff;;;CO)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemRoot%\Regedit.exe",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDrive%\pagefile.sys",1,"D:P(A;C:IOI;0x001200a9;;;SY)"  
"%SystemDirectory%\Rdisk.exe",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDirectory%\Ntbackup.exe",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDirectory%\Rcp.exe",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"

# UNCLASSIFIED

"%SystemDirectory%\Rsh.exe",2,"D:P(A;C:I O I ;0x001f01ff;;;DA)(A;C:I O I ;0x001f01ff;;;SY)"  
"%SystemDirectory%\Rexec.exe",2,"D:P(A;C:I O I ;0x001f01ff;;;DA)(A;C:I O I ;0x001f01ff;;;SY)"  
"%SystemDirectory%\Regedt32.exe",2,"D:P(A;C:I O I ;0x001f01ff;;;DA)(A;C:I O I ;0x001f01ff;;;SY)"  
"%SystemDirectory%\Regedt32.hlp",2,"D:P(A;C:I O I ;0x001f01ff;;;DA)(A;C:I O I ;0x001f01ff;;;SY)"  
"%SystemDirectory%\Regedt32.cnt",2,"D:P(A;C:I O I ;0x001f01ff;;;DA)(A;C:I O I ;0x001f01ff;;;SY)"  
"%SystemRoot%\Security",2,"D:P(A;C:I O I ;0x001f01ff;;;DA)(A;C:I O I ;0x001f01ff;;;SY)"  
"%SystemRoot%\Help",2,"D:P(A;C:I O I ;0x001f01ff;;;DA)(A;C:I O I ;0x001201bf;;;AU)(A;C:I O I ;0x001f01ff;;;CO)(A;C:I O I ;0x001f01ff;;;SY)"  
"%SystemRoot%\COOKIES",2,"D:P(A;C:I O I ;0x001f01ff;;;DA)(A;C:I O I ;0x001201bf;;;AU)(A;C:I O I ;0x001f01ff;;;CO)(A;C:I O I ;0x001f01ff;;;SY)"  
"%SystemRoot%\History",2,"D:P(A;C:I O I ;0x001f01ff;;;DA)(A;C:I O I ;0x001201bf;;;AU)(A;C:I O I ;0x001f01ff;;;CO)(A;C:I O I ;0x001f01ff;;;SY)"  
"%SystemRoot%\Temporary Internet Files",2,"D:P(A;C:I O I ;0x001f01ff;;;DA)(A;C:I O I ;0x001201bf;;;AU)(A;C:I O I ;0x001f01ff;;;CO)(A;C:I O I ;0x001f01ff;;;SY)"  
"%SystemRoot%\SendTo",2,"D:P(A;C:I O I ;0x001f01ff;;;DA)(A;C:I O I ;0x001201bf;;;AU)(A;C:I O I ;0x001f01ff;;;CO)(A;C:I O I ;0x001f01ff;;;SY)"  
[Privilege Rights]  
SeAssignPrimaryTokenPrivilege =  
SeAuditPrivilege =  
SeBackupPrivilege = Administrators,Backup Operators,Server Operators  
SeChangeNotifyPrivilege =  
SeCreatePagefilePrivilege = Administrators  
SeCreatePermanentPrivilege =  
SeCreateTokenPrivilege =  
SeDebugPrivilege =  
SeIncreaseBasePriorityPrivilege = Administrators  
SeIncreaseQuotaPrivilege =  
SeInteractiveLogonRight = Server Operators,Print Operators,Backup Operators,Administrators,Account Operators  
SeLoadDriverPrivilege = Administrators  
SeLockMemoryPrivilege =  
SeMachineAccountPrivilege =  
SeNetworkLogonRight = Administrators,Authenticated Users  
SeProfileSingleProcessPrivilege = Administrators  
SeRemoteShutdownPrivilege = Server Operators,Administrators  
SeRestorePrivilege = Server Operators,Backup Operators,Administrators  
SeSecurityPrivilege = Administrators  
SeShutdownPrivilege = Administrators  
SeSystemEnvironmentPrivilege = Administrators  
SeSystemProfilePrivilege = Administrators  
SeSystemTimePrivilege = Server Operators,Administrators  
SeTakeOwnershipPrivilege = Administrators  
SeBatchLogonRight =  
SeServiceLogonRight =  
SeTcbPrivilege =

UNCLASSIFIED

This Page Intentionally Left Blank

UNCLASSIFIED

**(U) BDC.inf**

## [System Access]

ForceLogoffWhenHourExpire = 1

## [System Log]

MaximumLogSize = 4194240

AuditLogRetentionPeriod = 2

RestrictGuestAccess = 1

## [Security Log]

MaximumLogSize = 4194240

AuditLogRetentionPeriod = 2

RestrictGuestAccess = 1

## [Application Log]

MaximumLogSize = 4194240

AuditLogRetentionPeriod = 2

RestrictGuestAccess = 1

## [Event Audit]

AuditSystemEvents = 3

AuditLogonEvents = 3

AuditObjectAccess = 2

AuditPrivilegeUse = 2

AuditPolicyChange = 3

AuditAccountManage = 3

AuditProcessTracking = 0

CrashOnAuditFull = 1

## [Version]

signature="\$CHICAGO\$"

## [Group Membership]

## [Service General Setting]

Schedule,4,"D:(A;;0x000200ad;;;DA)(A;;0x000201fd;;;SY)S:(SA;FA;0x000f01ff;;;WD)"

## [Registry Keys]

"MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg",2,"D:P(A;CI;0x000f003f;;DA)(A;CI;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Windows 3.1 Migration

Status",2,"D:P(A;CI;0x000f003f;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;SY)"

# UNCLASSIFIED

"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Microsoft\OS/2 Subsystem for NT",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"

"MACHINE\HARDWARE",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x0002001f;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"

"USERS\DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"

"USERS\DEFAULT\SOFTWARE\Microsoft\NetDDE",2,"D:P(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"

"USERS\DEFAULT",2,"D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon",2,"D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\IniFileMapping",2,"D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options",2,"D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontMapper",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Font Drivers",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Windows NT",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce",2,"D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Windows",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x0002001f;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Secure",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Rpc",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Ole",2,"D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;CO)(A;CI;0x10000000;;;SY)"

"MACHINE\SOFTWARE\Microsoft\NetDDE",2,"D:P(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Cryptography",2,"D:P(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)(A;CI;0x80000000;;;AU)"

"MACHINE\SOFTWARE\Classes",1,""

"CLASSES\_ROOT\helpfile",2,"D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"

"CLASSES\_ROOT",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x0002001f;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"

"MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Shares",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"

UNCLASSIFIED

"MACHINE\SYSTEM\CurrentControlSet\Services\Schedule",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"  
"MACHINE\SYSTEM\CurrentControlSet\Services\UPS",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"  
"USERS\DEFAULT\SOFTWARE\Microsoft\Protected Storage System Provider",1,""  
"MACHINE\SOFTWARE\Secure",2,"D:P(A;CI;0x10000000;;;CO)(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"  
"MACHINE\SOFTWARE\Program Groups",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\009",1,""  
"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Compatibility",2,"D:P(A;CI;0xc0000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;CO)(A;CI;0x10000000;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Protected Storage System Provider",1,""  
"MACHINE\SOFTWARE",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x0003001f;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"  
"CLASSES\_ROOT\hlp",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Shell Extensions",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"  
[File Security]  
"%SystemRoot%\mapiuid.ini",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001301bf;;;AU)(A;CI;0x001f01ff;;;CO)(A;CI;0x001f01ff;;;SY)"  
"%SystemRoot%\drwtsn32.log",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001301bf;;;AU)(A;CI;0x001f01ff;;;CO)(A;CI;0x001f01ff;;;SY)"  
"%SystemRoot%\nsreg.dat",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001301bf;;;AU)(A;CI;0x001f01ff;;;CO)(A;CI;0x001f01ff;;;SY)"  
"%SystemDirectory%\spool\Printers",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001301bf;;;AU)(A;CI;0x001f01ff;;;CO)(A;CI;0x001301bf;;;RP)(A;CI;0x001f01ff;;;SY)"  
"%SystemRoot%",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001200a9;;;AU)(A;CI;0x001f01ff;;;CO)(A;CI;0x001f01ff;;;SY)"  
"%SystemDirectory%",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001200a9;;;AU)(A;CI;0x001f01ff;;;CO)(A;CI;0x001f01ff;;;SY)"  
"%SystemRoot%\\$NtServicePackUninstall\$",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001f01ff;;;SY)"  
"%SystemDrive%",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001201bf;;;AU)(A;CI;0x001f01ff;;;CO)(A;CI;0x001f01ff;;;SY)"  
"%SystemDirectory%\repl\export",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001200a9;;;AU)(A;CI;0x001f01ff;;;CO)(A;CI;0x001200a9;;;RP)(A;CI;0x001f01ff;;;SY)"  
"%SystemDirectory%\repl\import",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001200a9;;;AU)(A;CI;0x001f01ff;;;CO)(A;CI;0x001301bf;;;RP)(A;CI;0x001f01ff;;;SY)"  
"%SystemDirectory%\config",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001f01ff;;;SY)"  
"%SystemRoot%\repair",2,"D:P(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"  
"%SystemDrive%\Program Files",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001201bf;;;AU)(A;CI;0x001f01ff;;;CO)(A;CI;0x001f01ff;;;SY)"  
"c:\config.sys",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001200a9;;;AU)(A;CI;0x001f01ff;;;SY)"  
"c:\autoexec.bat",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001200a9;;;AU)(A;CI;0x001f01ff;;;SY)"  
"c:\ntldr",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001f01ff;;;SY)"  
"c:\ntdetect.com",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001f01ff;;;SY)"  
"c:\boot.ini",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001f01ff;;;SY)"  
"%SystemDrive%\Users",1,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001201bf;;;AU)(A;CI;0x001f01ff;;;CO)(A;CI;0x001f01ff;;;S-0x1-0x000000000005-0x15-0x3b1e46f5-0x69bf70fb-0x253b7c20-0x200)(A;CI;0x001f01ff;;;SY)"

# UNCLASSIFIED

"%SystemDrive%\Win32app", 1, "D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001201bf;;;AU)(A;C:IOI;0x001f01ff;;;CO)(A;C:IOI;0x001f01ff;;;S-0x1-0x000000000005-0x15-0x3b1e46f5-0x69bf70fb-0x253b7c20-0x200)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemRoot%\Profiles", 1, "D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001201bf;;;AU)(A;C:IOI;0x001f01ff;;;CO)(A;C:IOI;0x001f01ff;;;S-0x1-0x000000000005-0x15-0x3b1e46f5-0x69bf70fb-0x253b7c20-0x200)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDrive%\Io.sys", 2, "D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001200a9;;;AU)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDrive%\ntldr", 2, "D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDrive%\Config.sys", 2, "D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001200a9;;;AU)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDrive%\Msdos.sys", 2, "D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001200a9;;;AU)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDrive%\Ntdetect.com", 2, "D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDrive%\boot.ini", 2, "D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDrive%\Autoexec.bat", 2, "D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001200a9;;;AU)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDrive%\NTReskit", 2, "D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001200a9;;;AU)(A;C:IOI;0x001f01ff;;;CO)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemRoot%\Regedit.exe", 2, "D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDrive%\pagefile.sys", 1, "D:P(A;C:IOI;0x001200a9;;;SY)"  
"%SystemDirectory%\Rdisk.exe", 2, "D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDirectory%\Ntbackup.exe", 2, "D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDirectory%\Rcp.exe", 2, "D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDirectory%\Rsh.exe", 2, "D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDirectory%\Rexec.exe", 2, "D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDirectory%\Regedt32.exe", 2, "D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDirectory%\Regedt32.hlp", 2, "D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDirectory%\Regedt32.cnt", 2, "D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemRoot%\Security", 2, "D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemRoot%\Help", 2, "D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001201bf;;;AU)(A;C:IOI;0x001f01ff;;;CO)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemRoot%\COOKIES", 2, "D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001201bf;;;AU)(A;C:IOI;0x001f01ff;;;CO)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemRoot%\History", 2, "D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001201bf;;;AU)(A;C:IOI;0x001f01ff;;;CO)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemRoot%\Temporary Internet Files", 2, "D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001201bf;;;AU)(A;C:IOI;0x001f01ff;;;CO)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemRoot%\SendTo", 2, "D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001201bf;;;AU)(A;C:IOI;0x001f01ff;;;CO)(A;C:IOI;0x001f01ff;;;SY)"

## [Registry Values]

MACHINE\System\CurrentControlSet\Services\Rdr\Parameters\EnablePlainTextPassword=4,0  
MACHINE\System\CurrentControlSet\Control\Session Manager\ProtectionMode=4,1  
MACHINE\System\CurrentControlSet\Control\Session Manager\Memory Management\ClearPageFileAtShutdown=4,1  
MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\AddPrintDrivers=4,1  
MACHINE\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel=4,1  
MACHINE\System\CurrentControlSet\Control\Lsa\CrashOnAuditFail=4,1  
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ShutdownWithoutLogon=1,0  
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\LegalNoticeText=1,.... <<< Message Text for Users Logging on >>> ....

# UNCLASSIFIED

MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\LegalNoticeCaption=1,.... <<<<  
Message Title for Users Logging on >>>> ....  
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\DontDisplayLastUserName=1,1  
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount=1,0  
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateFloppies=1,1  
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateCDRoms=1,1  
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon>PasswordExpiryWarning=15  
MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous=4,1  
MACHINE\System\CurrentControlSet\Control\Lsa\FullPrivilegeAuditing=3,30  
[Privilege Rights]  
SeNetworkLogonRight = Authenticated Users,Administrators  
SeTcbPrivilege =

UNCLASSIFIED

This Page Intentionally Left Blank

UNCLASSIFIED

## (U) MemberServer.inf

### [System Access]

MinimumPasswordAge = 1  
MaximumPasswordAge = 90  
MinimumPasswordLength = 12  
PasswordComplexity = 1  
PasswordHistorySize = 24  
LockoutBadCount = 3  
ResetLockoutCount = 15  
LockoutDuration = 15  
RequireLogonToChangePassword = 1  
ForceLogoffWhenHourExpire = 1

### [System Log]

MaximumLogSize = 4194240  
AuditLogRetentionPeriod = 2  
RestrictGuestAccess = 1

### [Security Log]

MaximumLogSize = 4194240  
AuditLogRetentionPeriod = 2  
RestrictGuestAccess = 1

### [Application Log]

MaximumLogSize = 4194240  
AuditLogRetentionPeriod = 2  
RestrictGuestAccess = 1

### [Event Audit]

AuditSystemEvents = 3  
AuditLogonEvents = 3  
AuditObjectAccess = 2  
AuditPrivilegeUse = 2  
AuditPolicyChange = 3  
AuditAccountManage = 3  
AuditProcessTracking = 0  
CrashOnAuditFull = 1

### [Version]

signature="\$CHICAGO\$"

### [Group Membership]

### [Service General Setting]

Schedule,4,"D:(A;;0x000200ad;;;DA)(A;;0x000201fd;;;SY)S:(SA;FA;0x000f01ff;;;WD)"

### [Registry Values]

# UNCLASSIFIED

MACHINE\System\CurrentControlSet\Control\Lsa\FullPrivilegeAuditing=3,30  
MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous=4,1  
MACHINE\Software\Microsoft\Windows  
NT\CurrentVersion\Winlogon>PasswordExpiryWarning=15  
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateCDRoms=1,1  
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateFloppies=1,1  
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount=1,0  
MACHINE\Software\Microsoft\Windows  
NT\CurrentVersion\Winlogon\DontDisplayLastUserName=1,1  
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\LegalNoticeCaption=1,....  
<<<< Message Title for Users Logging on >>>> ....  
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\LegalNoticeText=1,.... <<<<  
Message Text for Users Logging on >>> ....  
MACHINE\Software\Microsoft\Windows  
NT\CurrentVersion\Winlogon\ShutdownWithoutLogon=1,0  
MACHINE\System\CurrentControlSet\Control\Lsa\CrashOnAuditFail=4,1  
MACHINE\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel=4,1  
MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print  
Services\AddPrintDrivers=4,1  
MACHINE\System\CurrentControlSet\Control\Session Manager\Memory  
Management\ClearPageFileAtShutdown=4,1  
MACHINE\System\CurrentControlSet\Control\Session Manager\ProtectionMode=4,1  
MACHINE\System\CurrentControlSet\Services\Rdr\Parameters\EnablePlainTextPassword=4,0  
[Privilege Rights]  
SeAssignPrimaryTokenPrivilege =  
SeAuditPrivilege =  
SeBackupPrivilege = Administrators,Backup Operators,Server Operators  
SeChangeNotifyPrivilege =  
SeCreatePagefilePrivilege = Administrators  
SeCreatePermanentPrivilege =  
SeCreateTokenPrivilege =  
SeDebugPrivilege =  
SeIncreaseBasePriorityPrivilege = Administrators  
SeIncreaseQuotaPrivilege =  
SeInteractiveLogonRight = Server Operators,Print Operators,Backup  
Operators,Administrators,Account Operators  
SeLoadDriverPrivilege = Administrators  
SeLockMemoryPrivilege =  
SeMachineAccountPrivilege =  
SeNetworkLogonRight = Administrators,Authenticated Users  
SeProfileSingleProcessPrivilege = Administrators  
SeRemoteShutdownPrivilege = Server Operators,Administrators  
SeRestorePrivilege = Server Operators,Backup Operators,Administrators  
SeSecurityPrivilege = Administrators  
SeShutdownPrivilege = Administrators  
SeSystemEnvironmentPrivilege = Administrators  
SeSystemProfilePrivilege = Administrators  
SeSystemTimePrivilege = Server Operators,Administrators  
SeTakeOwnershipPrivilege = Administrators  
SeBatchLogonRight =  
SeServiceLogonRight =  
SeTcbPrivilege =

[Registry Keys]

# UNCLASSIFIED

"MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg",2,"D:P(A;Cl;0x000f003f;;;DA)(A;Cl;0x000f003f;;;SY)"  
"MACHINE\SOFTWARE\Windows 3.1 Migration Status",2,"D:P(A;Cl;0x000f003f;;;DA)(A;Cl;0x00020019;;;AU)(A;Cl;0x000f003f;;;CO)(A;Cl;0x000f003f;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx",2,"D:P(A;Cl;0x000f003f;;;DA)(A;Cl;0x00020019;;;AU)(A;Cl;0x000f003f;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones",2,"D:P(A;Cl;0x000f003f;;;DA)(A;Cl;0x00020019;;;AU)(A;Cl;0x000f003f;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run",2,"D:P(A;Cl;0x000f003f;;;DA)(A;Cl;0x00020019;;;AU)(A;Cl;0x000f003f;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\OS/2 Subsystem for NT",2,"D:P(A;Cl;0x000f003f;;;DA)(A;Cl;0x00020019;;;AU)(A;Cl;0x000f003f;;;CO)(A;Cl;0x000f003f;;;SY)"  
"MACHINE\HARDWARE",2,"D:P(A;Cl;0x000f003f;;;DA)(A;Cl;0x0002001f;;;AU)(A;Cl;0x000f003f;;;CO)(A;Cl;0x000f003f;;;SY)"  
"USERS\DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies",2,"D:P(A;Cl;0x000f003f;;;DA)(A;Cl;0x00020019;;;AU)(A;Cl;0x000f003f;;;CO)(A;Cl;0x000f003f;;;SY)"  
"USERS\DEFAULT\SOFTWARE\Microsoft\NetDDE",2,"D:P(A;Cl;0x10000000;;;DA)(A;Cl;0x10000000;;;SY)"  
"USERS\DEFAULT",2,"D:P(A;Cl;0x80000000;;;AU)(A;Cl;0x10000000;;;DA)(A;Cl;0x10000000;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon",2,"D:P(A;Cl;0x80000000;;;AU)(A;Cl;0x10000000;;;DA)(A;Cl;0x10000000;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib",2,"D:P(A;Cl;0x000f003f;;;DA)(A;Cl;0x00020019;;;AU)(A;Cl;0x000f003f;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\IniFileMapping",2,"D:P(A;Cl;0x80000000;;;AU)(A;Cl;0x10000000;;;DA)(A;Cl;0x10000000;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options",2,"D:P(A;Cl;0x80000000;;;AU)(A;Cl;0x10000000;;;DA)(A;Cl;0x10000000;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontMapper",2,"D:P(A;Cl;0x000f003f;;;DA)(A;Cl;0x00020019;;;AU)(A;Cl;0x000f003f;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Font Drivers",2,"D:P(A;Cl;0x000f003f;;;DA)(A;Cl;0x00020019;;;AU)(A;Cl;0x000f003f;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug",2,"D:P(A;Cl;0x000f003f;;;DA)(A;Cl;0x00020019;;;AU)(A;Cl;0x000f003f;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Windows NT",2,"D:P(A;Cl;0x000f003f;;;DA)(A;Cl;0x00020019;;;AU)(A;Cl;0x000f003f;;;CO)(A;Cl;0x000f003f;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce",2,"D:P(A;Cl;0x80000000;;;AU)(A;Cl;0x10000000;;;DA)(A;Cl;0x10000000;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Windows",2,"D:P(A;Cl;0x000f003f;;;DA)(A;Cl;0x0002001f;;;AU)(A;Cl;0x000f003f;;;CO)(A;Cl;0x000f003f;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Secure",2,"D:P(A;Cl;0x000f003f;;;DA)(A;Cl;0x00020019;;;AU)(A;Cl;0x000f003f;;;CO)(A;Cl;0x000f003f;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Rpc",2,"D:P(A;Cl;0x000f003f;;;DA)(A;Cl;0x00020019;;;AU)(A;Cl;0x000f003f;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Ole",2,"D:P(A;Cl;0x80000000;;;AU)(A;Cl;0x10000000;;;DA)(A;Cl;0x10000000;;;CO)(A;Cl;0x10000000;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\NetDDE",2,"D:P(A;Cl;0x10000000;;;DA)(A;Cl;0x10000000;;;SY)"

UNCLASSIFIED

# UNCLASSIFIED

"MACHINE\SOFTWARE\Microsoft\Cryptography",2,"D:P(A;CI;0x10000000;;;DA)(A;CI;0x100000000;;;SY)(A;CI;0x80000000;;;AU)"  
"MACHINE\SOFTWARE\Classes",1,""  
"CLASSES\_ROOT\helpfile",2,"D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x100000000;;;SY)"  
"CLASSES\_ROOT",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x0002001f;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"  
"MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Shares",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"  
"MACHINE\SYSTEM\CurrentControlSet\Services\Schedule",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"  
"MACHINE\SYSTEM\CurrentControlSet\Services\UPS",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"  
"USERS\DEFAULT\SOFTWARE\Microsoft\Protected Storage System Provider",1,""  
"MACHINE\SOFTWARE\Secure",2,"D:P(A;CI;0x10000000;;;CO)(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"  
"MACHINE\SOFTWARE\Program Groups",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\009",1,""  
"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Compatibility",2,"D:P(A;CI;0xc0000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;CO)(A;CI;0x10000000;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Protected Storage System Provider",1,""  
"MACHINE\SOFTWARE",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x0003001f;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"  
"CLASSES\_ROOT\hlp",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Shell Extensions",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"  
[File Security]  
"%SystemRoot%\mapiuid.ini",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001301bf;;;AU)(A;CI;0x001f01ff;;;CO)(A;CI;0x001f01ff;;;SY)"  
"%SystemRoot%\drwtsn32.log",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001301bf;;;AU)(A;CI;0x001f01ff;;;CO)(A;CI;0x001f01ff;;;SY)"  
"%SystemRoot%\nsreg.dat",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001301bf;;;AU)(A;CI;0x001f01ff;;;CO)(A;CI;0x001f01ff;;;SY)"  
"%SystemDirectory%\spool\Printers",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001301bf;;;AU)(A;CI;0x001f01ff;;;CO)(A;CI;0x001301bf;;;RP)(A;CI;0x001f01ff;;;SY)"  
"%SystemRoot%",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001200a9;;;AU)(A;CI;0x001f01ff;;;CO)(A;CI;0x001f01ff;;;SY)"  
"%SystemDirectory%",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001200a9;;;AU)(A;CI;0x001f01ff;;;CO)(A;CI;0x001f01ff;;;SY)"  
"%SystemRoot%\\$NtServicePackUninstall\$",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001f01ff;;;SY)"  
"%SystemDrive%",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001201bf;;;AU)(A;CI;0x001f01ff;;;CO)(A;CI;0x001f01ff;;;SY)"  
"%SystemDirectory%\repl\export",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001200a9;;;AU)(A;CI;0x001f01ff;;;CO)(A;CI;0x001200a9;;;RP)(A;CI;0x001f01ff;;;SY)"  
"%SystemDirectory%\repl\import",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001200a9;;;AU)(A;CI;0x001f01ff;;;CO)(A;CI;0x001301bf;;;RP)(A;CI;0x001f01ff;;;SY)"  
"%SystemDirectory%\config",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001f01ff;;;SY)"  
"%SystemRoot%\repair",2,"D:P(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"

# UNCLASSIFIED

"%SystemDrive%\Program Files",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001201bf;;;AU)(A;C:IOI;0x001f01ff;;;CO)(A;C:IOI;0x001f01ff;;;SY)"  
"c:\config.sys",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001200a9;;;AU)(A;C:IOI;0x001f01ff;;;SY)"  
"c:\autoexec.bat",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001200a9;;;AU)(A;C:IOI;0x001f01ff;;;SY)"  
"c:\ntldr",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"  
"c:\ntdetect.com",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"  
"c:\boot.ini",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDrive%\Users",1,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001201bf;;;AU)(A;C:IOI;0x001f01ff;;;CO)(A;C:IOI;0x001f01ff;;;S-0x1-0x0000000000005-0x15-0x3b1e46f5-0x69bf70fb-0x253b7c20-0x200)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDrive%\Win32app",1,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001201bf;;;AU)(A;C:IOI;0x001f01ff;;;CO)(A;C:IOI;0x001f01ff;;;S-0x1-0x0000000000005-0x15-0x3b1e46f5-0x69bf70fb-0x253b7c20-0x200)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemRoot%\Profiles",1,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001201bf;;;AU)(A;C:IOI;0x001f01ff;;;CO)(A;C:IOI;0x001f01ff;;;S-0x1-0x0000000000005-0x15-0x3b1e46f5-0x69bf70fb-0x253b7c20-0x200)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDrive%\io.sys",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001200a9;;;AU)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDrive%\ntldr",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDrive%\Config.sys",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001200a9;;;AU)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDrive%\Msdos.sys",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001200a9;;;AU)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDrive%\Ntdetect.com",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDrive%\boot.ini",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDrive%\Autoexec.bat",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001200a9;;;AU)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDrive%\NTReskit",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001200a9;;;AU)(A;C:IOI;0x001f01ff;;;CO)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemRoot%\Regedit.exe",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDrive%\pagefile.sys",1,"D:P(A;C:IOI;0x001200a9;;;SY)"  
"%SystemDirectory%\Rdisk.exe",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDirectory%\Ntbackup.exe",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDirectory%\Rcp.exe",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDirectory%\Rsh.exe",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDirectory%\Rexec.exe",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDirectory%\Regedt32.exe",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDirectory%\Regedt32.hlp",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemDirectory%\Regedt32.cnt",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemRoot%\Security",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemRoot%\Help",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001201bf;;;AU)(A;C:IOI;0x001f01ff;;;CO)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemRoot%\COOKIES",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001201bf;;;AU)(A;C:IOI;0x001f01ff;;;CO)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemRoot%\History",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001201bf;;;AU)(A;C:IOI;0x001f01ff;;;CO)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemRoot%\Temporary Internet Files",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001201bf;;;AU)(A;C:IOI;0x001f01ff;;;CO)(A;C:IOI;0x001f01ff;;;SY)"  
"%SystemRoot%\SendTo",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001201bf;;;AU)(A;C:IOI;0x001f01ff;;;CO)(A;C:IOI;0x001f01ff;;;SY)"

UNCLASSIFIED

This Page Intentionally Left Blank

UNCLASSIFIED

## (U) Workstation.inf

### [System Access]

MinimumPasswordAge = 1  
MaximumPasswordAge = 90  
MinimumPasswordLength = 12  
PasswordComplexity = 1  
PasswordHistorySize = 24  
LockoutBadCount = 3  
ResetLockoutCount = 15  
LockoutDuration = 15  
RequireLogonToChangePassword = 1  
ForceLogoffWhenHourExpire = 1

### [System Log]

MaximumLogSize = 4194240  
AuditLogRetentionPeriod = 2  
RestrictGuestAccess = 1

### [Security Log]

MaximumLogSize = 4194240  
AuditLogRetentionPeriod = 2  
RestrictGuestAccess = 1

### [Application Log]

MaximumLogSize = 4194240  
AuditLogRetentionPeriod = 2  
RestrictGuestAccess = 1

### [Event Audit]

AuditSystemEvents = 3  
AuditLogonEvents = 3  
AuditObjectAccess = 2  
AuditPrivilegeUse = 2  
AuditPolicyChange = 3  
AuditAccountManage = 3  
AuditProcessTracking = 0  
CrashOnAuditFull = 1

### [Version]

signature="\$CHICAGO\$"

### [Group Membership]

### [Service General Setting]

Schedule,4,"D:(A;;0x000200ad;;;DA)(A;;0x000201fd;;;SY)S:(SA;FA;0x000f01ff;;;WD)"

### [Registry Values]

# UNCLASSIFIED

MACHINE\System\CurrentControlSet\Control\Lsa\FullPrivilegeAuditing=3,30  
MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous=4,1  
MACHINE\Software\Microsoft\Windows  
NT\CurrentVersion\Winlogon>PasswordExpiryWarning=15  
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateCDRoms=1,1  
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateFloppies=1,1  
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount=1,0  
MACHINE\Software\Microsoft\Windows  
NT\CurrentVersion\Winlogon\DontDisplayLastUserName=1,1  
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\LegalNoticeCaption=1,....  
<<<< Message Title for Users Logging on >>>> ....  
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\LegalNoticeText=1,.... <<<  
Message Text for Users Logging on >>> ....  
MACHINE\Software\Microsoft\Windows  
NT\CurrentVersion\Winlogon\ShutdownWithoutLogon=1,0  
MACHINE\System\CurrentControlSet\Control\Lsa\CrashOnAuditFail=4,1  
MACHINE\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel=4,1  
MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print  
Services\AddPrintDrivers=4,1  
MACHINE\System\CurrentControlSet\Control\Session Manager\Memory  
Management\ClearPageFileAtShutdown=4,1  
MACHINE\System\CurrentControlSet\Control\Session Manager\ProtectionMode=4,1  
MACHINE\System\CurrentControlSet\Services\Rdr\Parameters\EnablePlainTextPassword=4,0

## [Registry Keys]

"MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x000f003f;;;SY)"  
"MACHINE\SOFTWARE\Windows 3.1 Migration  
Status",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time  
Zones",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\OS/2 Subsystem for  
NT",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"  
"MACHINE\HARDWARE",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x0002001f;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"  
"USERS\DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"  
"USERS\DEFAULT\SOFTWARE\Microsoft\NetDDE",2,"D:P(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"  
"USERS\DEFAULT",2,"D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\Winlogon",2,"D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\Perflib",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\IniFileMapping",2,"D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"

# UNCLASSIFIED

"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options",2,"D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontMapper",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Font Drivers",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Windows NT",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce",2,"D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Windows",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x0002001f;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Secure",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Rpc",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Ole",2,"D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;CO)(A;CI;0x10000000;;;SY)"

"MACHINE\SOFTWARE\Microsoft\NetDDE",2,"D:P(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Cryptography",2,"D:P(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)(A;CI;0x80000000;;;AU)"

"MACHINE\SOFTWARE\Classes",1,""

"CLASSES\_ROOT\helpfile",2,"D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"

"CLASSES\_ROOT",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x0002001f;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"

"MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Shares",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"

"MACHINE\SYSTEM\CurrentControlSet\Services\Schedule",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"

"MACHINE\SYSTEM\CurrentControlSet\Services\UPS",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"

"USERS\DEFAULT\SOFTWARE\Microsoft\Protected Storage System Provider",1,""

"MACHINE\SOFTWARE\Secure",2,"D:P(A;CI;0x10000000;;;CO)(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"

"MACHINE\SOFTWARE\Program Groups",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\009",1,""

"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Compatibility",2,"D:P(A;CI;0xc0000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;CO)(A;CI;0x10000000;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Protected Storage System Provider",1,""

"MACHINE\SOFTWARE",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x0003001f;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"

"CLASSES\_ROOT\hlp",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Shell Extensions",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"

UNCLASSIFIED

"MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"  
[File Security]  
"%SystemRoot%\mapiuid.ini",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001301bf;;;AU)(A;CI;0x001f01ff;;;CO)(A;CI;0x001f01ff;;;SY)"  
"%SystemRoot%\drwtsn32.log",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001301bf;;;AU)(A;CI;0x001f01ff;;;CO)(A;CI;0x001f01ff;;;SY)"  
"%SystemRoot%\nsreg.dat",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001301bf;;;AU)(A;CI;0x001f01ff;;;CO)(A;CI;0x001f01ff;;;SY)"  
"%SystemDirectory%\spool\Printers",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001301bf;;;AU)(A;CI;0x001f01ff;;;CO)(A;CI;0x001301bf;;;RP)(A;CI;0x001f01ff;;;SY)"  
"%SystemRoot%",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001200a9;;;AU)(A;CI;0x001f01ff;;;CO)(A;CI;0x001f01ff;;;SY)"  
"%SystemDirectory%",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001200a9;;;AU)(A;CI;0x001f01ff;;;CO)(A;CI;0x001f01ff;;;SY)"  
"%SystemRoot%\\$NtServicePackUninstall\$",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001f01ff;;;SY)"  
"%SystemDrive%",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001201bf;;;AU)(A;CI;0x001f01ff;;;CO)(A;CI;0x001f01ff;;;SY)"  
"%SystemDirectory%\repl\export",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001200a9;;;AU)(A;CI;0x001f01ff;;;CO)(A;CI;0x001200a9;;;RP)(A;CI;0x001f01ff;;;SY)"  
"%SystemDirectory%\repl\import",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001200a9;;;AU)(A;CI;0x001f01ff;;;CO)(A;CI;0x001301bf;;;RP)(A;CI;0x001f01ff;;;SY)"  
"%SystemDirectory%\config",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001f01ff;;;SY)"  
"%SystemRoot%\repair",2,"D:P(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"  
"%SystemDrive%\Program Files",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001201bf;;;AU)(A;CI;0x001f01ff;;;CO)(A;CI;0x001f01ff;;;SY)"  
"c:\config.sys",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001200a9;;;AU)(A;CI;0x001f01ff;;;SY)"  
"c:\autoexec.bat",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001200a9;;;AU)(A;CI;0x001f01ff;;;SY)"  
"c:\ntldr",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001f01ff;;;SY)"  
"c:\ntdetect.com",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001f01ff;;;SY)"  
"c:\boot.ini",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001f01ff;;;SY)"  
"%SystemDrive%\Users",1,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001201bf;;;AU)(A;CI;0x001f01ff;;;CO)(A;CI;0x001f01ff;;;S-0x1-0x0000000000005-0x15-0x3b1e46f5-0x69bf70fb-0x253b7c20-0x200)(A;CI;0x001f01ff;;;SY)"  
"%SystemDrive%\Win32app",1,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001201bf;;;AU)(A;CI;0x001f01ff;;;CO)(A;CI;0x001f01ff;;;S-0x1-0x0000000000005-0x15-0x3b1e46f5-0x69bf70fb-0x253b7c20-0x200)(A;CI;0x001f01ff;;;SY)"  
"%SystemRoot%\Profiles",1,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001201bf;;;AU)(A;CI;0x001f01ff;;;CO)(A;CI;0x001f01ff;;;S-0x1-0x0000000000005-0x15-0x3b1e46f5-0x69bf70fb-0x253b7c20-0x200)(A;CI;0x001f01ff;;;SY)"  
"%SystemDrive%\lo.sys",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001200a9;;;AU)(A;CI;0x001f01ff;;;SY)"  
"%SystemDrive%\ntldr",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001f01ff;;;SY)"  
"%SystemDrive%\Config.sys",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001200a9;;;AU)(A;CI;0x001f01ff;;;SY)"  
"%SystemDrive%\Msdos.sys",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001200a9;;;AU)(A;CI;0x001f01ff;;;SY)"  
"%SystemDrive%\Ntdetect.com",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001f01ff;;;SY)"  
"%SystemDrive%\boot.ini",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001f01ff;;;SY)"  
"%SystemDrive%\Autoexec.bat",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001200a9;;;AU)(A;CI;0x001f01ff;;;SY)"  
"%SystemDrive%\NTRReskit",2,"D:P(A;CI;0x001f01ff;;;DA)(A;CI;0x001200a9;;;AU)(A;CI;0x001f01ff;;;CO)(A;CI;0x001f01ff;;;SY)"

# UNCLASSIFIED

"%SystemRoot%\Regedit.exe",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001f01ff;;;SY)"  
"%SystemDrive%\pagefile.sys",1,"D:P(A;CIOI;0x001200a9;;;SY)"  
"%SystemDirectory%\Rdisk.exe",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001f01ff;;;SY)"  
"%SystemDirectory%\Ntbackup.exe",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001f01ff;;;SY)"  
"%SystemDirectory%\Rcp.exe",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001f01ff;;;SY)"  
"%SystemDirectory%\Rsh.exe",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001f01ff;;;SY)"  
"%SystemDirectory%\Rexec.exe",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001f01ff;;;SY)"  
"%SystemDirectory%\Regedt32.exe",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001f01ff;;;SY)"  
"%SystemDirectory%\Regedt32.hlp",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001f01ff;;;SY)"  
"%SystemDirectory%\Regedt32.cnt",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001f01ff;;;SY)"  
"%SystemRoot%\Security",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001f01ff;;;SY)"  
"%SystemRoot%\Help",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001201bf;;;AU)(A;CIOI;0x001f01ff;;;CO)(A;CIOI;0x001f01ff;;;SY)"  
"%SystemRoot%\COOKIES",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001201bf;;;AU)(A;CIOI;0x001f01ff;;;CO)(A;CIOI;0x001f01ff;;;SY)"  
"%SystemRoot%\History",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001201bf;;;AU)(A;CIOI;0x001f01ff;;;CO)(A;CIOI;0x001f01ff;;;SY)"  
"%SystemRoot%\Temporary Internet Files",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001201bf;;;AU)(A;CIOI;0x001f01ff;;;CO)(A;CIOI;0x001f01ff;;;SY)"  
"%SystemRoot%\SendTo",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001201bf;;;AU)(A;CIOI;0x001f01ff;;;CO)(A;CIOI;0x001f01ff;;;SY)"  
[Privilege Rights]  
SeAssignPrimaryTokenPrivilege =  
SeAuditPrivilege =  
SeBackupPrivilege = Backup Operators,Administrators  
SeChangeNotifyPrivilege =  
SeCreatePagefilePrivilege = Administrators  
SeCreatePermanentPrivilege =  
SeCreateTokenPrivilege =  
SeDebugPrivilege =  
SeIncreaseBasePriorityPrivilege = Administrators  
SeIncreaseQuotaPrivilege =  
SeInteractiveLogonRight = Authenticated Users,Administrators  
SeLoadDriverPrivilege = Administrators  
SeLockMemoryPrivilege =  
SeMachineAccountPrivilege =  
SeNetworkLogonRight = Authenticated Users,Administrators  
SeProfileSingleProcessPrivilege = Administrators  
SeRemoteShutdownPrivilege = Administrators  
SeRestorePrivilege = Backup Operators,Administrators  
SeSecurityPrivilege = Administrators  
SeShutdownPrivilege = Authenticated Users,Administrators  
SeSystemEnvironmentPrivilege = Administrators  
SeSystemProfilePrivilege = Administrators  
SeSystemTimePrivilege = Administrators  
SeTakeOwnershipPrivilege = Administrators  
SeBatchLogonRight =  
SeServiceLogonRight =  
SeTcbPrivilege =

UNCLASSIFIED

This Page Intentionally Left Blank

UNCLASSIFIED

## (U) Exchange.inf

(U) Refer to Microsoft's Exchange publications for backup and restoration procedures and follow those procedures before installing any configuration (.inf) files on the Exchange Server.

**(U) WARNING: Before installing this file on an existing Microsoft Exchange server it is imperative to back up all configuration related files and mail boxes. If possible install Microsoft Exchange after securing a Member Server.**

### Exchange Server 5.0 and 5.5 Installation

- If the Exchange Server is installed in the default partition (same as the operating system). The default permissions applied to the %SystemDrive% directory by the OS guide will not allow installation of the Exchange Server to a directory under the %SystemDrive% directory. If necessary to install the Exchange Server on the same partition as the OS, simply create the destination directory before beginning and give the Exchange services account "**Full Control**".
- Change the permissions associated with the file %SystemRoot%\SYSTEM32\mapisvc.inf to allow the "Authenticated Users" group Modify access.

### Client Installation (Outlook 97, Outlook 98, Exchange Client)

- Give "Authenticated Users" Modify access to the file %SystemRoot%\forms\frmcache.dat. This change is necessary for the clients to function properly.
- In an environment where multiple people share the same workstation, it is probable that multiple user mail profiles will be created on a single machine. If this happens, file access errors can occur when using the Exchange Client or Outlook 97 client if multiple users select the same name for their profiles as a consequence of the tightened file permissions associated with the OS guide. To avoid this problem, user profiles should be given unique names. A suggested method for insuring this is to use the account name in the profile such as "%account name% outlook".
- In order for Outlook users (non admins) to use encrypted RPC between client and server, authenticated users need read access on Registry key Machine/Software/Microsoft/RPC and all subkeys.

This is not an issue when using Outlook 98 due to differences in the manner in which the profiles are stored.

For additional information on setting up Mail boxes using Internet Explorer see **AccessMail.txt** on the Companion CD.

The following is the Exchange.inf security configuration file:

```
[System Access]
MinimumPasswordAge = 1
```

# UNCLASSIFIED

MaximumPasswordAge = 90  
MinimumPasswordLength = 12  
PasswordComplexity = 1  
PasswordHistorySize = 24  
LockoutBadCount = 3  
ResetLockoutCount = 15  
LockoutDuration = 15  
RequireLogonToChangePassword = 1  
ForceLogoffWhenHourExpire = 1

## [System Log]

MaximumLogSize = 4194240  
AuditLogRetentionPeriod = 2  
RestrictGuestAccess = 1

## [Security Log]

MaximumLogSize = 4194240  
AuditLogRetentionPeriod = 2  
RestrictGuestAccess = 1

## [Application Log]

MaximumLogSize = 4194240  
AuditLogRetentionPeriod = 2  
RestrictGuestAccess = 1

## [Event Audit]

AuditSystemEvents = 3  
AuditLogonEvents = 3  
AuditObjectAccess = 2  
AuditPrivilegeUse = 2  
AuditPolicyChange = 3  
AuditAccountManage = 3  
AuditProcessTracking = 0  
CrashOnAuditFull = 1

## [Version]

signature="\$CHICAGO\$"

## [Group Membership]

## [Service General Setting]

Schedule,4,"D:(A;;0x000200ad;;;DA)(A;;0x000201fd;;;SY)S:(SA;FA;0x000f01ff;;;WD)"

## [Registry Values]

MACHINE\System\CurrentControlSet\Control\Lsa\FullPrivilegeAuditing=3,30  
MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous=4,1  
MACHINE\Software\Microsoft\Windows  
NT\CurrentVersion\Winlogon>PasswordExpiryWarning=15  
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateCDRoms=1,1  
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateFloppies=1,1  
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount=1,0  
MACHINE\Software\Microsoft\Windows  
NT\CurrentVersion\Winlogon\DontDisplayLastUserName=1,1  
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\LegalNoticeCaption=1,....  
<<<< Message Title for Users Logging on >>>> ....

# UNCLASSIFIED

MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\LegalNoticeText=1,.... <<<  
Message Text for Users Logging on >>> ....  
MACHINE\Software\Microsoft\Windows  
NT\CurrentVersion\Winlogon\ShutdownWithoutLogon=1,0  
MACHINE\System\CurrentControlSet\Control\Lsa\CrashOnAuditFail=4,1  
MACHINE\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel=4,1  
MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print  
Services\AddPrintDrivers=4,1  
MACHINE\System\CurrentControlSet\Control\Session Manager\Memory  
Management\ClearPageFileAtShutdown=4,1  
MACHINE\System\CurrentControlSet\Control\Session Manager\ProtectionMode=4,1  
MACHINE\System\CurrentControlSet\Services\Rdr\Parameters\EnablePlainTextPassword=4,0

## [Privilege Rights]

SeAssignPrimaryTokenPrivilege =  
SeAuditPrivilege =  
SeBackupPrivilege = Server Operators,Backup Operators,Administrators  
SeChangeNotifyPrivilege =  
SeCreatePagefilePrivilege = Administrators  
SeCreatePermanentPrivilege =  
SeCreateTokenPrivilege =  
SeDebugPrivilege =  
SeIncreaseBasePriorityPrivilege = Administrators  
SeIncreaseQuotaPrivilege =  
SeInteractiveLogonRight = Administrators  
SeLoadDriverPrivilege = Administrators  
SeLockMemoryPrivilege =  
SeMachineAccountPrivilege =  
SeNetworkLogonRight = Authenticated Users,Administrators  
SeProfileSingleProcessPrivilege = Administrators  
SeRemoteShutdownPrivilege = Administrators  
SeRestorePrivilege = Backup Operators,Administrators  
SeSecurityPrivilege = Administrators  
SeShutdownPrivilege = Administrators  
SeSystemEnvironmentPrivilege = Administrators  
SeSystemProfilePrivilege = Administrators  
SeSystemTimePrivilege = Administrators  
SeTakeOwnershipPrivilege = Administrators  
SeBatchLogonRight =  
SeServiceLogonRight =  
SeTcbPrivilege =

## [Registry Keys]

"MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall",2,"D:P(A;CI;0x000f003f;;;D  
A)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Shell  
Extensions",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x  
000f003f;;;SY)"  
"CLASSES\_ROOT\hlp",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;  
SY)"  
"MACHINE\SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\Compatibility",2,"D:P(A;CI;0xc0000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x1  
0000000;;;CO)(A;CI;0x10000000;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\009",1,""  
"MACHINE\SOFTWARE\Secure",2,"D:P(A;CI;0x10000000;;;CO)(A;CI;0x80000000;;;AU)(A;CI;0x  
10000000;;;DA)(A;CI;0x10000000;;;SY)"  
"USERS\DEFAULT\SOFTWARE\Microsoft\Protected Storage System Provider",1,""

UNCLASSIFIED

# UNCLASSIFIED

"MACHINE\SYSTEM\CurrentControlSet\Services\UPS",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"  
"MACHINE\SYSTEM\CurrentControlSet\Services\Schedule",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"  
"MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Shares",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"  
"CLASSES\_ROOT",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x0002001f;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"  
"CLASSES\_ROOT\helpfile",2,"D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Cryptography",2,"D:P(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)(A;CI;0x80000000;;;AU)"  
"MACHINE\SOFTWARE\Microsoft\NetDDE",2,"D:P(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Ole",2,"D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;CO)(A;CI;0x10000000;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Rpc",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Secure",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce",2,"D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Windows NT",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Font Drivers",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontMapper",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options",2,"D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\IniFileMapping",2,"D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon",2,"D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"  
"USERS\DEFAULT",2,"D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"  
"USERS\DEFAULT\SOFTWARE\Microsoft\NetDDE",2,"D:P(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"  
"USERS\DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"  
"MACHINE\HARDWARE",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x0002001f;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"  
"MACHINE\SOFTWARE\Microsoft\OS/2 Subsystem for NT",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"

# UNCLASSIFIED

"MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Windows 3.1 Migration Status",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"

"MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x000f003f;;;SY)"

[File Security]

"%SystemRoot%\SendTo",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001201bf;;;AU)(A;CIOI;0x001f01ff;;;CO)(A;CIOI;0x001f01ff;;;SY)"

"%SystemRoot%\Temporary Internet Files",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001201bf;;;AU)(A;CIOI;0x001f01ff;;;CO)(A;CIOI;0x001f01ff;;;SY)"

"%SystemRoot%\History",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001201bf;;;AU)(A;CIOI;0x001f01ff;;;CO)(A;CIOI;0x001f01ff;;;SY)"

"%SystemRoot%\COOKIES",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001201bf;;;AU)(A;CIOI;0x001f01ff;;;CO)(A;CIOI;0x001f01ff;;;SY)"

"%SystemRoot%\Help",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001201bf;;;AU)(A;CIOI;0x001f01ff;;;CO)(A;CIOI;0x001f01ff;;;SY)"

"%SystemRoot%\Security",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001f01ff;;;SY)"

"%SystemDirectory%\Regedt32.cnt",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001f01ff;;;SY)"

"%SystemDirectory%\Regedt32.hlp",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001f01ff;;;SY)"

"%SystemDirectory%\Regedt32.exe",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001f01ff;;;SY)"

"%SystemDirectory%\Rexec.exe",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001f01ff;;;SY)"

"%SystemDirectory%\Rsh.exe",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001f01ff;;;SY)"

"%SystemDirectory%\Rcp.exe",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001f01ff;;;SY)"

"%SystemDirectory%\Ntbackup.exe",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001f01ff;;;SY)"

"%SystemDirectory%\Rdisk.exe",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001f01ff;;;SY)"

"%SystemDrive%\pagefile.sys",1,"D:P(A;CIOI;0x001200a9;;;SY)"

"%SystemRoot%\Regedit.exe",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001f01ff;;;SY)"

"%SystemDrive%\NTReskit",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001200a9;;;AU)(A;CIOI;0x001f01ff;;;CO)(A;CIOI;0x001f01ff;;;SY)"

"%SystemDrive%\Autoexec.bat",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001200a9;;;AU)(A;CIOI;0x001f01ff;;;SY)"

"%SystemDrive%\boot.ini",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001f01ff;;;SY)"

"%SystemDrive%\Ntdetect.com",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001f01ff;;;SY)"

"%SystemDrive%\Msdos.sys",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001200a9;;;AU)(A;CIOI;0x001f01ff;;;SY)"

"%SystemDrive%\Config.sys",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001200a9;;;AU)(A;CIOI;0x001f01ff;;;SY)"

"%SystemDrive%\ntldr",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001f01ff;;;SY)"

"%SystemDrive%\lo.sys",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001200a9;;;AU)(A;CIOI;0x001f01ff;;;SY)"

"%SystemRoot%\Profiles",1,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001201bf;;;AU)(A;CIOI;0x001f01ff;;;CO)(A;CIOI;0x001f01ff;;;S-0x1-0x000000000005-0x15-0x3b1e46f5-0x69bf70fb-0x253b7c20-0x200)(A;CIOI;0x001f01ff;;;SY)"

"%SystemDrive%\Win32app",1,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001201bf;;;AU)(A;CIOI;0x001f01ff;;;CO)(A;CIOI;0x001f01ff;;;S-0x1-0x000000000005-0x15-0x3b1e46f5-0x69bf70fb-0x253b7c20-0x200)(A;CIOI;0x001f01ff;;;SY)"

"%SystemDrive%\Users",1,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001201bf;;;AU)(A;CIOI;0x001f01ff;;;CO)(A;CIOI;0x001f01ff;;;S-0x1-0x000000000005-0x15-0x3b1e46f5-0x69bf70fb-0x253b7c20-0x200)(A;CIOI;0x001f01ff;;;SY)"

# UNCLASSIFIED

"c:\boot.ini",2,"D:P(A;C;I;O;I;0x001f01ff;;;DA)(A;C;I;O;I;0x001f01ff;;;SY)"  
"c:\ntdetect.com",2,"D:P(A;C;I;O;I;0x001f01ff;;;DA)(A;C;I;O;I;0x001f01ff;;;SY)"  
"c:\ntldr",2,"D:P(A;C;I;O;I;0x001f01ff;;;DA)(A;C;I;O;I;0x001f01ff;;;SY)"  
"c:\autoexec.bat",2,"D:P(A;C;I;O;I;0x001f01ff;;;DA)(A;C;I;O;I;0x001200a9;;;AU)(A;C;I;O;I;0x001f01ff;;;SY)"  
"c:\config.sys",2,"D:P(A;C;I;O;I;0x001f01ff;;;DA)(A;C;I;O;I;0x001200a9;;;AU)(A;C;I;O;I;0x001f01ff;;;SY)"  
"%SystemDrive%\Program Files",2,"D:P(A;C;I;O;I;0x001f01ff;;;DA)(A;C;I;O;I;0x001201bf;;;AU)(A;C;I;O;I;0x001f01ff;;;CO)(A;C;I;O;I;0x001f01ff;;;SY)"  
"%SystemRoot%\repair",2,"D:P(A;C;I;O;I;0x10000000;;;DA)(A;C;I;O;I;0x10000000;;;SY)"  
"%SystemDirectory%\config",2,"D:P(A;C;I;O;I;0x001f01ff;;;DA)(A;C;I;O;I;0x001f01ff;;;SY)"  
"%SystemDirectory%\repl\import",2,"D:P(A;C;I;O;I;0x001f01ff;;;DA)(A;C;I;O;I;0x001200a9;;;AU)(A;C;I;O;I;0x001f01ff;;;CO)(A;C;I;O;I;0x001301bf;;;RP)(A;C;I;O;I;0x001f01ff;;;SY)"  
"%SystemDirectory%\repl\export",2,"D:P(A;C;I;O;I;0x001f01ff;;;DA)(A;C;I;O;I;0x001200a9;;;AU)(A;C;I;O;I;0x001f01ff;;;CO)(A;C;I;O;I;0x001200a9;;;RP)(A;C;I;O;I;0x001f01ff;;;SY)"  
"%SystemDrive%",2,"D:P(A;C;I;O;I;0x001f01ff;;;DA)(A;C;I;O;I;0x001201bf;;;AU)(A;C;I;O;I;0x001f01ff;;;CO)(A;C;I;O;I;0x001f01ff;;;SY)"  
"%SystemRoot%\\$NtServicePackUninstall\$",2,"D:P(A;C;I;O;I;0x001f01ff;;;DA)(A;C;I;O;I;0x001f01ff;;;SY)"  
"%SystemDirectory%",2,"D:P(A;C;I;O;I;0x001f01ff;;;DA)(A;C;I;O;I;0x001200a9;;;AU)(A;C;I;O;I;0x001f01ff;;;CO)(A;C;I;O;I;0x001f01ff;;;SY)"  
"%SystemRoot%",2,"D:P(A;C;I;O;I;0x001f01ff;;;DA)(A;C;I;O;I;0x001200a9;;;AU)(A;C;I;O;I;0x001f01ff;;;CO)(A;C;I;O;I;0x001f01ff;;;SY)"  
"%SystemDirectory%\spool\Printers",2,"D:P(A;C;I;O;I;0x001f01ff;;;DA)(A;C;I;O;I;0x001301bf;;;AU)(A;C;I;O;I;0x001f01ff;;;CO)(A;C;I;O;I;0x001301bf;;;RP)(A;C;I;O;I;0x001f01ff;;;SY)"  
"%SystemRoot%\nsreg.dat",2,"D:P(A;C;I;O;I;0x001f01ff;;;DA)(A;C;I;O;I;0x001301bf;;;AU)(A;C;I;O;I;0x001f01ff;;;CO)(A;C;I;O;I;0x001f01ff;;;SY)"  
"%SystemRoot%\drwtsn32.log",2,"D:P(A;C;I;O;I;0x001f01ff;;;DA)(A;C;I;O;I;0x001301bf;;;AU)(A;C;I;O;I;0x001f01ff;;;CO)(A;C;I;O;I;0x001f01ff;;;SY)"  
"%SystemRoot%\mapiuid.ini",2,"D:P(A;C;I;O;I;0x001f01ff;;;DA)(A;C;I;O;I;0x001301bf;;;AU)(A;C;I;O;I;0x001f01ff;;;CO)(A;C;I;O;I;0x001f01ff;;;SY)"  
"%SystemDrive%\EXCHSRVR",1,"D:P(A;C;I;O;I;0x001f01ff;;;DA)(A;C;I;O;I;0x001301bf;;;AU)(A;C;I;O;I;0x001f01ff;;;CO)(A;C;I;O;I;0x001f01ff;;;SY)"

## (U) IIS\_Sample.inf

(U) This is a sample IIS file and needs to be changed for site specific needs.

```
[System Access]
MinimumPasswordAge = 1
MaximumPasswordAge = 90
MinimumPasswordLength = 12
PasswordComplexity = 1
PasswordHistorySize = 24
LockoutBadCount = 3
ResetLockoutCount = 15
LockoutDuration = 15
RequireLogonToChangePassword = 1
ForceLogoffWhenHourExpire = 1
```

```
[System Log]
MaximumLogSize = 4194240
AuditLogRetentionPeriod = 2
RestrictGuestAccess = 1
```

```
[Security Log]
MaximumLogSize = 4194240
AuditLogRetentionPeriod = 2
RestrictGuestAccess = 1
```

```
[Application Log]
MaximumLogSize = 4194240
AuditLogRetentionPeriod = 2
RestrictGuestAccess = 1
```

```
[Event Audit]
AuditSystemEvents = 3
AuditLogonEvents = 3
AuditObjectAccess = 2
AuditPrivilegeUse = 2
AuditPolicyChange = 3
AuditAccountManage = 3
AuditProcessTracking = 0
CrashOnAuditFull = 1
```

```
[Version]
signature="$CHICAGO$"
```

```
[Group Membership]
```

# UNCLASSIFIED

[Service General Setting]

Schedule,4,"D:(A;;0x000200ad;;;DA)(A;;0x000201fd;;;SY)S:(SA;FA;0x000f01ff;;;WD)"

[Registry Values]

MACHINE\System\CurrentControlSet\Control\Lsa\FullPrivilegeAuditing=3,30

MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous=4,1

MACHINE\Software\Microsoft\Windows

NT\CurrentVersion\Winlogon>PasswordExpiryWarning=15

MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateCDRoms=1,1

MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateFloppies=1,1

MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount=1,0

MACHINE\Software\Microsoft\Windows

NT\CurrentVersion\Winlogon\DontDisplayLastUserName=1,1

MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\LegalNoticeCaption=1,....

<<<< Message Title for Users Logging on >>>> ....

MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\LegalNoticeText=1,.... <<<

Message Text for Users Logging on >>> ....

MACHINE\Software\Microsoft\Windows

NT\CurrentVersion\Winlogon\ShutdownWithoutLogon=1,0

MACHINE\System\CurrentControlSet\Control\Lsa\CrashOnAuditFail=4,1

MACHINE\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel=4,1

MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print

Services\AddPrintDrivers=4,1

MACHINE\System\CurrentControlSet\Control\Session Manager\Memory

Management\ClearPageFileAtShutdown=4,1

MACHINE\System\CurrentControlSet\Control\Session Manager\ProtectionMode=4,1

MACHINE\System\CurrentControlSet\Services\Rdr\Parameters\EnablePlainTextPassword=4,0

[Registry Keys]

"MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Windows 3.1 Migration

Status",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time

Zones",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Microsoft\OS/2 Subsystem for

NT",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"

"MACHINE\HARDWARE",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x0002001f;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"

"USERS\DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"

"USERS\DEFAULT\SOFTWARE\Microsoft\NetDDE",2,"D:P(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"

"USERS\DEFAULT",2,"D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Windows

NT\CurrentVersion\Winlogon",2,"D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Windows

NT\CurrentVersion\Perflib",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;SY)"

# UNCLASSIFIED

"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\IniFileMapping",2,"D:P(A;Cl;0x80000000;;;AU)(A;Cl;0x10000000;;;DA)(A;Cl;0x10000000;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options",2,"D:P(A;Cl;0x80000000;;;AU)(A;Cl;0x10000000;;;DA)(A;Cl;0x10000000;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontMapper",2,"D:P(A;Cl;0x000f003f;;;DA)(A;Cl;0x00020019;;;AU)(A;Cl;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Font Drivers",2,"D:P(A;Cl;0x000f003f;;;DA)(A;Cl;0x00020019;;;AU)(A;Cl;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug",2,"D:P(A;Cl;0x000f003f;;;DA)(A;Cl;0x00020019;;;AU)(A;Cl;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Windows NT",2,"D:P(A;Cl;0x000f003f;;;DA)(A;Cl;0x00020019;;;AU)(A;Cl;0x000f003f;;;CO)(A;Cl;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce",2,"D:P(A;Cl;0x80000000;;;AU)(A;Cl;0x10000000;;;DA)(A;Cl;0x10000000;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Windows",2,"D:P(A;Cl;0x000f003f;;;DA)(A;Cl;0x0002001f;;;AU)(A;Cl;0x000f003f;;;CO)(A;Cl;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Secure",2,"D:P(A;Cl;0x000f003f;;;DA)(A;Cl;0x00020019;;;AU)(A;Cl;0x000f003f;;;CO)(A;Cl;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Rpc",2,"D:P(A;Cl;0x000f003f;;;DA)(A;Cl;0x00020019;;;AU)(A;Cl;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Ole",2,"D:P(A;Cl;0x80000000;;;AU)(A;Cl;0x10000000;;;DA)(A;Cl;0x10000000;;;CO)(A;Cl;0x10000000;;;SY)"

"MACHINE\SOFTWARE\Microsoft\NetDDE",2,"D:P(A;Cl;0x10000000;;;DA)(A;Cl;0x10000000;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Cryptography",2,"D:P(A;Cl;0x10000000;;;DA)(A;Cl;0x10000000;;;SY)(A;Cl;0x80000000;;;AU)"

"MACHINE\SOFTWARE\Classes",1,""

"CLASSES\_ROOT\helpfile",2,"D:P(A;Cl;0x80000000;;;AU)(A;Cl;0x10000000;;;DA)(A;Cl;0x10000000;;;SY)"

"CLASSES\_ROOT",2,"D:P(A;Cl;0x000f003f;;;DA)(A;Cl;0x0002001f;;;AU)(A;Cl;0x000f003f;;;CO)(A;Cl;0x000f003f;;;SY)"

"MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Shares",2,"D:P(A;Cl;0x000f003f;;;DA)(A;Cl;0x00020019;;;AU)(A;Cl;0x000f003f;;;CO)(A;Cl;0x000f003f;;;SY)"

"MACHINE\SYSTEM\CurrentControlSet\Services\Schedule",2,"D:P(A;Cl;0x000f003f;;;DA)(A;Cl;0x00020019;;;AU)(A;Cl;0x000f003f;;;CO)(A;Cl;0x000f003f;;;SY)"

"MACHINE\SYSTEM\CurrentControlSet\Services\UPS",2,"D:P(A;Cl;0x000f003f;;;DA)(A;Cl;0x00020019;;;AU)(A;Cl;0x000f003f;;;CO)(A;Cl;0x000f003f;;;SY)"

"USERS\DEFAULT\SOFTWARE\Microsoft\Protected Storage System Provider",1,""

"MACHINE\SOFTWARE\Secure",2,"D:P(A;Cl;0x10000000;;;CO)(A;Cl;0x80000000;;;AU)(A;Cl;0x10000000;;;DA)(A;Cl;0x10000000;;;SY)"

"MACHINE\SOFTWARE\Program Groups",2,"D:P(A;Cl;0x000f003f;;;DA)(A;Cl;0x00020019;;;AU)(A;Cl;0x000f003f;;;CO)(A;Cl;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\009",1,""

"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Compatibility",2,"D:P(A;Cl;0xc0000000;;;AU)(A;Cl;0x10000000;;;DA)(A;Cl;0x10000000;;;CO)(A;Cl;0x10000000;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Protected Storage System Provider",1,""

"MACHINE\SOFTWARE",2,"D:P(A;Cl;0x000f003f;;;DA)(A;Cl;0x0003001f;;;AU)(A;Cl;0x000f003f;;;CO)(A;Cl;0x000f003f;;;SY)"

"CLASSES\_ROOT\hip",2,"D:P(A;Cl;0x000f003f;;;DA)(A;Cl;0x00020019;;;AU)(A;Cl;0x000f003f;;;SY)"

UNCLASSIFIED

# UNCLASSIFIED

```
"MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Shell
Extensions",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x
000f003f;;;SY)"
"MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall",2,"D:P(A;CI;0x000f003f;;;D
A)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"
[Privilege Rights]
SeAssignPrimaryTokenPrivilege =
SeAuditPrivilege =
SeBackupPrivilege = Server Operators,Backup Operators,Administrators
SeChangeNotifyPrivilege =
SeCreatePagefilePrivilege = Administrators
SeCreatePermanentPrivilege =
SeCreateTokenPrivilege =
SeDebugPrivilege =
SeIncreaseBasePriorityPrivilege = Administrators
SeIncreaseQuotaPrivilege =
SeInteractiveLogonRight = Account Operators,Administrators,Backup Operators,Print
Operators,Server Operators
SeLoadDriverPrivilege = Administrators
SeLockMemoryPrivilege =
SeMachineAccountPrivilege =
SeNetworkLogonRight = TEST\IWAM_DELL,TEST\IUSR_DELL,Authenticated
Users,Administrators
SeProfileSingleProcessPrivilege = Administrators
SeRemoteShutdownPrivilege = Administrators,Server Operators
SeRestorePrivilege = Administrators,Backup Operators,Server Operators
SeSecurityPrivilege = Administrators
SeShutdownPrivilege = Administrators
SeSystemEnvironmentPrivilege = Administrators
SeSystemProfilePrivilege = Administrators
SeSystemTimePrivilege = Administrators,Server Operators
SeTakeOwnershipPrivilege = Administrators
SeBatchLogonRight =
SeServiceLogonRight =
SeTcbPrivilege =
[File Security]
"%SystemDrive%\inetpub\ftproot",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001200a9;;;AU)(A;CI
OI;0x001201bf;;;IU)(A;CIOI;0x001200a9;;;S-0x1-0x000000000005-0x15-0x3b1e46f5-0x69bf70fb-
0x253b7c20-0x3f8)(A;CIOI;0x001f01ff;;;S-0x1-0x000000000005-0x15-0x3b1e46f5-0x69bf70fb-
0x253b7c20-0x3fa)"
"%SystemDrive%\inetpub\mailroot",2,"D:P(A;CIOI;0x001200a9;;;DA)(A;CIOI;0x001200a9;;;AU)(A
;CIOI;0x001200a9;;;IU)(A;CIOI;0x001201bf;;;S-0x1-0x000000000005-0x15-0x3b1e46f5-
0x69bf70fb-0x253b7c20-0x3f8)(A;CIOI;0x001f01ff;;;S-0x1-0x000000000005-0x15-0x3b1e46f5-
0x69bf70fb-0x253b7c20-0x3fa)"
"%SystemDrive%\inetpub\mail",2,"D:P(A;CIOI;0x001200a9;;;DA)(A;CIOI;0x001200a9;;;AU)(A;CI
OI;0x001200a9;;;IU)(A;CIOI;0x001200a9;;;S-0x1-0x000000000005-0x15-0x3b1e46f5-0x69bf70fb-
0x253b7c20-0x3f8)(A;CIOI;0x001f01ff;;;S-0x1-0x000000000005-0x15-0x3b1e46f5-0x69bf70fb-
0x253b7c20-0x3fa)"
"%SystemDrive%\inetpub\nttpfile\drop",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001200a9;;;IU)(
A;CIOI;0x001200a9;;;S-0x1-0x000000000005-0x15-0x3b1e46f5-0x69bf70fb-0x253b7c20-
0x3f8)(A;CIOI;0x001f01ff;;;S-0x1-0x000000000005-0x15-0x3b1e46f5-0x69bf70fb-0x253b7c20-
0x3fa)"
"%SystemDrive%\inetpub\scripts",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001200a9;;;S-0x1-
0x000000000005-0x15-0x3b1e46f5-0x69bf70fb-0x253b7c20-0x3f8)(A;CIOI;0x001f01ff;;;S-0x1-
0x000000000005-0x15-0x3b1e46f5-0x69bf70fb-0x253b7c20-0x3fa)"
```

UNCLASSIFIED

"%SystemDrive%\inetpub\wwwroot",2,"D:P(A;C:IOI;0x001200a9;;;IU)(A;C:IOI;0x001200a9;;;S-0x1-0x0000000000005-0x15-0x3b1e46f5-0x69bf70fb-0x253b7c20-0x3f8)(A;C:IOI;0x001f01ff;;;S-0x1-0x0000000000005-0x15-0x3b1e46f5-0x69bf70fb-0x253b7c20-0x3fa)"

"%SystemDrive%\inetpub",2,"D:P(A;C:IOI;0x001200a9;;;AU)(A;C:IOI;0x001301bf;;;IU)(A;C:IOI;0x001200a9;;;S-0x1-0x0000000000005-0x15-0x3b1e46f5-0x69bf70fb-0x253b7c20-0x3f8)(A;C:IOI;0x001f01ff;;;S-0x1-0x0000000000005-0x15-0x3b1e46f5-0x69bf70fb-0x253b7c20-0x3fa)"

"%SystemRoot%\SendTo",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001201bf;;;AU)(A;C:IOI;0x001f01ff;;;CO)(A;C:IOI;0x001f01ff;;;SY)"

"%SystemRoot%\Temporary Internet Files",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001201bf;;;AU)(A;C:IOI;0x001f01ff;;;CO)(A;C:IOI;0x001f01ff;;;SY)"

"%SystemRoot%\History",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001201bf;;;AU)(A;C:IOI;0x001f01ff;;;CO)(A;C:IOI;0x001f01ff;;;SY)"

"%SystemRoot%\COOKIES",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001201bf;;;AU)(A;C:IOI;0x001f01ff;;;CO)(A;C:IOI;0x001f01ff;;;SY)"

"%SystemRoot%\Help",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001201bf;;;AU)(A;C:IOI;0x001f01ff;;;CO)(A;C:IOI;0x001f01ff;;;SY)"

"%SystemRoot%\Security",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"

"%SystemDirectory%\Regedt32.cnt",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"

"%SystemDirectory%\Regedt32.hlp",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"

"%SystemDirectory%\Regedt32.exe",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"

"%SystemDirectory%\Rexec.exe",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"

"%SystemDirectory%\Rsh.exe",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"

"%SystemDirectory%\Rcp.exe",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"

"%SystemDirectory%\Ntbackup.exe",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"

"%SystemDirectory%\Rdisk.exe",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"

"%SystemDrive%\pagefile.sys",1,"D:P(A;C:IOI;0x001200a9;;;SY)"

"%SystemRoot%\Regedit.exe",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"

"%SystemDrive%\NTRReskit",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001200a9;;;AU)(A;C:IOI;0x001f01ff;;;CO)(A;C:IOI;0x001f01ff;;;SY)"

"%SystemDrive%\Autoexec.bat",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001200a9;;;AU)(A;C:IOI;0x001f01ff;;;SY)"

"%SystemDrive%\boot.ini",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"

"%SystemDrive%\Ntdetect.com",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"

"%SystemDrive%\Msdos.sys",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001200a9;;;AU)(A;C:IOI;0x001f01ff;;;SY)"

"%SystemDrive%\Config.sys",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001200a9;;;AU)(A;C:IOI;0x001f01ff;;;SY)"

"%SystemDrive%\ntldr",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"

"%SystemDrive%\Io.sys",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001200a9;;;AU)(A;C:IOI;0x001f01ff;;;SY)"

"%SystemRoot%\Profiles",1,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001201bf;;;AU)(A;C:IOI;0x001f01ff;;;CO)(A;C:IOI;0x001f01ff;;;S-0x1-0x0000000000005-0x15-0x3b1e46f5-0x69bf70fb-0x253b7c20-0x200)(A;C:IOI;0x001f01ff;;;SY)"

"%SystemDrive%\Win32app",1,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001201bf;;;AU)(A;C:IOI;0x001f01ff;;;CO)(A;C:IOI;0x001f01ff;;;S-0x1-0x0000000000005-0x15-0x3b1e46f5-0x69bf70fb-0x253b7c20-0x200)(A;C:IOI;0x001f01ff;;;SY)"

"%SystemDrive%\Users",1,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001201bf;;;AU)(A;C:IOI;0x001f01ff;;;CO)(A;C:IOI;0x001f01ff;;;S-0x1-0x0000000000005-0x15-0x3b1e46f5-0x69bf70fb-0x253b7c20-0x200)(A;C:IOI;0x001f01ff;;;SY)"

"c:\boot.ini",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"

"c:\ntdetect.com",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"

"c:\ntldr",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001f01ff;;;SY)"

"c:\autoexec.bat",2,"D:P(A;C:IOI;0x001f01ff;;;DA)(A;C:IOI;0x001200a9;;;AU)(A;C:IOI;0x001f01ff;;;SY)"

# UNCLASSIFIED

```
"c:\config.sys",2,"D:P(A;CLOI;0x001f01ff;;;DA)(A;CLOI;0x001200a9;;;AU)(A;CLOI;0x001f01ff;;;SY)"
"%SystemDrive%\Program
Files",2,"D:P(A;CLOI;0x001f01ff;;;DA)(A;CLOI;0x001201bf;;;AU)(A;CLOI;0x001f01ff;;;CO)(A;CLOI;0
x001f01ff;;;SY)"
"%SystemRoot%\repair",2,"D:P(A;CLOI;0x10000000;;;DA)(A;CLOI;0x10000000;;;SY)"
"%SystemDirectory%\config",2,"D:P(A;CLOI;0x001f01ff;;;DA)(A;CLOI;0x001f01ff;;;SY)"
"%SystemDirectory%\repl\import",2,"D:P(A;CLOI;0x001f01ff;;;DA)(A;CLOI;0x001200a9;;;AU)(A;CLOI;0x001f01ff;;;CO)(A;CLOI;0x001301bf;;;RP)(A;CLOI;0x001f01ff;;;SY)"
"%SystemDirectory%\repl\export",2,"D:P(A;CLOI;0x001f01ff;;;DA)(A;CLOI;0x001200a9;;;AU)(A;CLOI;0x001f01ff;;;CO)(A;CLOI;0x001200a9;;;RP)(A;CLOI;0x001f01ff;;;SY)"
"%SystemDrive%",2,"D:P(A;CLOI;0x001f01ff;;;DA)(A;CLOI;0x001201bf;;;AU)(A;CLOI;0x001f01ff;;;CO)(A;CLOI;0x001f01ff;;;SY)"
"%SystemRoot%\$NtServicePackUninstall$",2,"D:P(A;CLOI;0x001f01ff;;;DA)(A;CLOI;0x001f01ff;;;SY)"
"%SystemDirectory%",2,"D:P(A;CLOI;0x001f01ff;;;DA)(A;CLOI;0x001200a9;;;AU)(A;CLOI;0x001f01ff;;;CO)(A;CLOI;0x001f01ff;;;SY)"
"%SystemRoot%",2,"D:P(A;CLOI;0x001f01ff;;;DA)(A;CLOI;0x001200a9;;;AU)(A;CLOI;0x001f01ff;;;CO)(A;CLOI;0x001f01ff;;;SY)"
"%SystemDirectory%\spool\Printers",2,"D:P(A;CLOI;0x001f01ff;;;DA)(A;CLOI;0x001301bf;;;AU)(A;CLOI;0x001f01ff;;;CO)(A;CLOI;0x001301bf;;;RP)(A;CLOI;0x001f01ff;;;SY)"
"%SystemRoot%\nsreg.dat",2,"D:P(A;CLOI;0x001f01ff;;;DA)(A;CLOI;0x001301bf;;;AU)(A;CLOI;0x001f01ff;;;CO)(A;CLOI;0x001f01ff;;;SY)"
"%SystemRoot%\drwtsn32.log",2,"D:P(A;CLOI;0x001f01ff;;;DA)(A;CLOI;0x001301bf;;;AU)(A;CLOI;0x001f01ff;;;CO)(A;CLOI;0x001f01ff;;;SY)"
"%SystemRoot%\mapiuid.ini",2,"D:P(A;CLOI;0x001f01ff;;;DA)(A;CLOI;0x001301bf;;;AU)(A;CLOI;0x001f01ff;;;CO)(A;CLOI;0x001f01ff;;;SY)"
[Profile Description]
Description=IIS Sample .INF (Site specific Information needed to be added)
```

## **(U) Microsoft Windows 95/98 Client Information**

(U) There is little that can be done to secure a Windows 95/98 client on an NT network from someone that has physical access to the computer. However, as a client computer, it can be rendered safe if some basic precautions are taken.

(U) System Administrators need to determine the type of exposure or risk that certain clients potentially have, and develop a security policy that reflects this level of risk. On the basis of that analysis, choose products, network technology, and practices for the installation, integration, and management of the network.

(U) Before Windows 95/98 clients are integrated into the network security model, consider the following issues:

### **(U) What kind of logon security is needed?**

(U) Are users allowed to log on to Windows 95/98 clients and the network with the same password? Should the network security provider validate users before being able to log on to a Windows 95/98 client? For both Windows 95 and 98, system policies can be used to require validation by a Windows NT server before allowing access to Windows 95/98 and to specify other Windows 95/98 password restrictions.

### **(U) What kind of resource protection is needed on Microsoft networks?**

(U) Before peer resource sharing is enabled, decide how to protect those resources with share-level or user-level security. User-level security provides greater security because the network security provider must authenticate the user name and password before access to the resource is granted.

(U) If shared files are required, give read-only access to just the needed directories, assign a strong password, and turn off sharing when it is no longer required.

(U) To understand more about controlling access to information on Windows 95/98 clients, read the Access Control topics in the Windows 95 and Windows 98 help file index.

**WARNING:** Since Windows 95 and 98 do not use NTFS and therefore can not implement secure shares, it is recommended that file and print sharing on Windows 95/98 clients be disabled.

### **(U) What kinds of access rights will users have to resources protected by user-level security?**

(U) Share-level security for Windows 95/98 clients allows only two choices of access control for shared directories: read-only or full control. User-level security in Windows 95/98 clients is more granular allowing more detailed access restrictions on shared directories. In addition to the read-only and full control options, users can specify individually: read, write, create, delete, change file attributes, directory list, and change access control permissions.

## UNCLASSIFIED

(U) Specify the types of rights users or groups of users have to resources by setting sharing properties for the shared resource (such as a folder or drive). For example, restrict other users to read-only access to files or give them read-access and write-access to files.

### **(U) How is user-level security enabled?**

(U) Enable security in a setup script or in system policies. If user-level security is enabled in either a setup script or through the Control Panel, remote administration is enabled by default for domain administrators on a Windows NT network.

### **(U) Should password caching be allowed?**

System policies can be used to disable password caching and thus require users to type a password each time they access a password-protected resource. When a user first types and saves a password when connecting to a password-protected resource, Windows 95/98 caches the password in the password list file. Logging on with a Windows 95/98 password unlocks the password list file and associates those passwords with the Windows 95/98 password. To the user, it seems as if the passwords for Windows 95/98 and for password-protected resources are the same. If password caching is disabled, users must type the password each time they connect to a password-protected resource.

### **(U) Should users be able to change Control Panel settings?**

(U) System policies can be used to restrict users' ability to change the configuration of system components, their desktops, applications, or network connections in the Control Panel folder.

### **(U) Does a client hard disk need extra protection?**

(U) Windows 95/98 security obstructs hacking over the network; but if a person has physical access to the computer, critical data can be taken from the hard disk by using Safe Mode or a floppy disk to start the workstation. If specific data requires greater levels of security, store critical files on a secure server. If computers require greater levels of security, Windows NT Workstation is recommended, because it provides a means to protect resources on a hard disk based on a user's identity.

### **(U) Are there applications that should not be run?**

(U) Access may need to be restricted to some applications while supplying access to other applications in the system. To implement this type of security, use system policies

### **(U) Do certain processes of an application need protection?**

(U) Do certain processes require additional security? If there is a need to further secure a distributed application, use DCOM. DCOM provides the structure to share applications at the component level between a server and clients. The components can be shared over the Internet or an Intranet. Using DCOM to set a security level for the application automatically applies that security level to each component, wherever located.

### **(U) Other system policy issues.**

- (U) Define policies to prevent users from enabling peer resource sharing services and to enforce other security components, such as preventing users from configuring system components

## UNCLASSIFIED

- (U) Install Windows 95 Service Pack 1. Available at <http://www.microsoft.com/windows95/downloads/>
- (U) To determine if the service pack is already installed on the client computer, click the Start Menu and choose Settings, Control Panel. Double-click the System icon and click the General tab. Locate the version number under the System heading. If the version number is 4.00.950 with no letters, SP1 will need to be installed. If the version number ends in an a or b, then the service pack is already installed.
- (U) Purchase the Windows 95 and 98 Resource Kits from Microsoft. The Resource Kits have many tools that will ease management and building a sound security configuration of these clients.

UNCLASSIFIED

This Page Intentionally Left Blank

UNCLASSIFIED

---

## **(U) Example Logon Banner**

(U) The DoD uses a standard warning banner that can be downloaded by using a web browser to view The United States Navy INFOSEC WebSite Server (<http://infosec.nosc.mil/infosec.html>). Select the text under the United States Department of Defense Warning Statement and copy it to the clipboard. This banner should resemble the following message:

(U) "This is a Department of Defense computer system. This computer system, including all related equipment, networks and network devices (specifically including Internet access), are provided only for authorized U. S. Government use. DoD computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored. Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal or adverse action. Use of this system constitutes consent to monitoring for these purposes."

(U) Windows NT displays a message box with a caption and text that can be configured before a user logs on to the machine. The DoD requires organizations to use this message box to display a warning that notifies users that they can be held legally liable if they attempt to log on without authorization to use the computer. The absence of such a notice could be construed as an invitation, without restriction, to log on to the machine and browse the system.

UNCLASSIFIED

This Page Intentionally Left Blank

UNCLASSIFIED

---

## (U) References

- Coopers & Lybrand L.L.P., *Microsoft Windows NT Server: Security Features and Future Direction*, July, 1997.
- Dalton, Wayne, et. al., *Windows NT Server 4: Security, Troubleshooting and Optimization*, Indianapolis, IN: New Riders Publishing, 1996.
- Microsoft TechNet, January 1999
- Microsoft Web Site, <http://www.microsoft.com>
- National Computer Security Center, *Microsoft Windows NT Version 3.5 Final Evaluation Report*, June 1995.
- Russel, Charlie and Sharon Crawford, *Running Microsoft Windows NT Server 4.0*, Redmond, Washington: Microsoft Press, 1997.
- Rutstein, Charles B., *Windows NT Security: A Practical Guide to Securing Windows NT Servers & Workstations*, New York: McGraw-Hill, 1997.
- Sheldon, Tom, *Windows NT Security Handbook: Everything You Need to Know to Protect Your Network*, Berkely, California: McGraw-Hill, 1997
- Stuple, Stuart J., ed., *Microsoft Windows NT Workstation Resource Kit: Comprehensive Resource Guide and Utilities for Windows NT Workstation Version 4.0*, Redmond, Washington: Microsoft Press, 1996.
- Stuple, Stuart J., ed., *Microsoft Windows NT Server Networking Guide: Technical Information and Tools for the Support Professional*, Redmond, Washington: Microsoft Press, 1996.
- Stuple, Stuart J., ed., *Microsoft Windows NT Server Resource Guide: Technical Information and Tools for the Support Professional*, Redmond, Washington: Microsoft Press, 1996.
- Thomas, Steven B., *Windows NT 4.0 Registry: A Professional Reference*, New York: McGraw-Hill, 1998