



# Secure Windows NT Installation and Configuration Guide

Windows NT for Navy IT-21

Version 1.3



**December 1998**

Department of the Navy  
Space and Naval Warfare Systems Command  
Naval Information Systems Security Office, PMW 161



## **Abstract**

The objective of this project is to provide the Navy with clear and concise implementation guidance for the secure installation and configuration of the Windows NT 4.0 server and workstation operating systems (OS). This guidance is based on the Navy IT-21 standard and is specific to the Naval Tactical Command Support System (NTCSS) and Joint Maritime Command Information System (JMCIS) local area network (LAN) architectures.

This guide covers pre-installation, server and workstation OS installation, and post-installation steps for securing a Windows NT domain. The post-installation portion includes instructions for C2 configuration, auditing, securing the registry, managing the file system, creating system policies and user profiles, controlling user accounts and rights, maintaining system repair data, and installing current service packs and hotfixes.

**Keywords:** Secure Windows NT 4.0 Configuration Guide Navy IT-21

## **Acknowledgments**

We would like to thank the following people for their contributions:

CAPT Daniel Galik, Program Manager, and Dave Mihelcic of SPAWAR PMW 161 for project impetus and funding.

Principle Authors/Researchers: Raymond P. Galloni, Jean-Paul F. Otin, Russell C. Reopell, Lara M. Sosnosky.

Michelle J. Gosselin and Thomas A. Gregg for project guidance and editing the content and style of the guide.

Linda C. Chock, Kenneth G. Jones, and Harvey H. Rubinovitz for contributing to the guide and editing content and style of the guide.

Carol R. Oakes for editing the content and style of the guide.

# Table of Contents

<b>Section</b>	<b>Page</b>
<b>1 Introduction</b>	<b>1-1</b>
1.1 Purpose	1-1
1.2 Scope	1-1
1.3 Background	1-1
1.4 Document Structure	1-2
1.5 Naming Conventions	1-3
<b>2 Pre-Installation</b>	<b>2-1</b>
<b>3 Blue Screen Installation</b>	<b>3-1</b>
<b>4 Graphical Window Installation</b>	<b>4-1</b>
<b>5 C2 Configuration Manager</b>	<b>5-1</b>
5.1 Background	5-1
5.2 C2 Overview	5-2
5.3 Preliminary Steps for C2 Configuration	5-2
5.4 Setting Up a C2-Compliant System	5-6
5.4.1 File Systems and OS Configuration	5-8
5.4.2 OS/2 Subsystem Configuration	5-8
5.4.3 Posix Subsystem Configuration	5-9
5.4.4 Security Log Configuration	5-10
5.4.5 Halt on Audit Failure	5-11
5.4.6 Displaying a Legal Notice Before Log On	5-12
5.4.7 Last Username Display	5-14
5.4.8 Shutdown Button	5-15
5.4.9 Password Length	5-16
5.4.10 Guest Account	5-17
5.4.11 Networking	5-17
5.4.12 Drive Letters and Printers	5-18
5.4.13 Removable Media Drives	5-19
5.4.14 Registry Security	5-19
5.4.15 File System Security	5-21
5.4.16 Other Security Items	5-21
<b>6 File System Configuration</b>	<b>6-1</b>
<b>7 Audit Policy Configuration</b>	<b>7-1</b>

<b>Section</b>	<b>Page</b>
<b>8 Registry Configuration</b>	<b>8-1</b>
<b>9 User Manager for Domains Configuration</b>	<b>9-1</b>
<b>10 User Account Policy Configuration</b>	<b>10-1</b>
<b>11 User Rights Policy Configuration</b>	<b>11-1</b>
<b>12 Domain Model Configuration (Trust Relationships)</b>	<b>12-1</b>
<b>13 User Environment Profile Configuration</b>	<b>13-1</b>
<b>14 System Policy Configuration</b>	<b>14-1</b>
<b>15 Control Panel Configuration</b>	<b>15-1</b>
<b>16 Miscellaneous Configurations</b>	<b>16-1</b>
<b>17 System Repair Data</b>	<b>17-1</b>
<b>Bibliography</b>	<b>BI-1</b>
<b>Appendix A Hotfixes</b>	<b>A-1</b>
<b>Appendix B Administrative Checklist</b>	<b>B-1</b>
<b>Glossary</b>	<b>GL-1</b>
<b>Distribution List</b>	<b>DI-1</b>

## List of Figures

<b>Figure</b>		<b>Page</b>
5-1	Virtual Memory Window	5-5
5-2	C2 Configuration Manager Main Menu	5-7
5-3	C2 Configuration - OS/2 Subsystem Window	5-9
5-4	C2 Configuration - OS/2 Subsystem Warning Window	5-9
5-5	C2 Configuration - Posix Subsystem Window	5-10
5-6	C2 Configuration – Posix Subsystem Warning Window	5-10
5-7	C2 Configuration – Security Log Settings Window	5-11
5-8	C2 Configuration - Audit Failure Settings Window	5-12
5-9	C2 Configuration - Logon Message Window	5-13
5-10	C2 Configuration - Logon Message Alert	5-13
5-11	C2 Configuration – Logon Message with Message Text	5-14
5-12	C2 Configuration – Last Username Display Window	5-15
5-13	C2 Configuration - Shutdown Button Window	5-16
5-14	C2 Configuration – Password Length Window	5-17
5-15	C2 Configuration - Networking Window	5-18
5-16	C2 Configuration - Drivers and Printers Window	5-18
5-17	C2 Configuration - Allocate Removable Drives Window	5-19
5-18	C2 Configuration - Registry ACLs Warning Window	5-20
5-19	C2 Configuration - Registry ACLs Window	5-20

<b>Figure</b>	<b>Page</b>
5-20 Warning Message: System Process - Low on Registry Quota	5-20
5-21 C2 Configuration - File System ACLs Warning Window	5-21
5-22 C2 Configuration - File System ACLs	5-21
5-23 C2 Configuration - Other Security Items Window	5-22
5-24 C2 Configuration Manager Main Menu	5-23
5-25 C2 Configuration Manager Restart Message Window	5-24
6-1 Windows NT Exploring Window	6-5
6-2 Sharing Properties Window	6-8
6-3 Directory Permissions Window	6-12
7-1 Audit Policy Window	7-2
8-1 Registry Editor Window	8-1
9-1 User Manager Window	9-3
9-2 New Global Group Window	9-4
9-3 New User Window	9-4
10-1 Account Policy Window	10-4
11-1 User Rights Policy Window	11-2
12-1 Trust Relationships Window	12-3
13-1 Windows NT Explorer - “%systemroot%\Profiles” Folder	13-5
13-2 Window NT Explorer - Initial Permissions on Profiles Folder	13-7
13-3 Windows NT Explorer - Final Permissions on Profiles Folder	13-9
14-1 Default Computer Properties - Network	14-3

<b>Figure</b>		<b>Page</b>
14-2	Default Computer System and Windows NT Networking Properties	14-4
14-3	Default Computer Properties - Windows NT Shell	14-7
14-4	Default Computer Properties - Windows NT System	14-8
14-5	Default Computer Properties - Windows NT User Profiles	14-9
14-6	System Policy Editor	14-10
14-7	System Policy Editor - Add Group Dialog Box	14-11
14-8	Domain Users Properties - Control Panel	14-12
14-9	Domain Users Properties - Shell	14-13
14-10	Domain Users Properties - System	14-16
14-11	Domain Users Properties - Windows NT Shell/Custom Folders	14-17
14-12	Domain Users Properties - Windows NT Shell/Restrictions	14-18
14-13	Domain Users Properties - Windows NT System	14-19
14-14	System Policy Editor - Group Priority	14-25
14-15	Server Manager Window	14-29
15-1	TCP/IP Properties Box	15-3
17-1	Run Window	17-3

## List of Tables

<b>Table</b>	<b>Page</b>
2-1 System Configuration Information	2-2
3-1 Blue Screen Installation Procedures	3-1
4-1 Graphical Window Installation Procedures for NT Server	4-1
4-2 Graphical Window Installation Procedures for NT Workstation	4-11
5-1 Pre-C2 Configuration Procedures	5-3
6-1 Windows NT File and Directory Permissions	6-1
6-2 File System Configuration Procedures	6-4
7-1 Audit Policy Configuration Procedures	7-1
7-2 Archiving and Securing Audit Logs	7-5
8-1 Registry Configuration Procedures	8-2
9-1 User Manager for Domains Configuration Procedures	9-1
10-1 Account Policy Configuration Procedures	10-2
11-1 User Rights Policy Configuration Procedures	11-1
11-2 User Rights Policy for NT Servers	11-2
11-3 User Rights Policy for NT Workstations	11-5
12-1 Domain Model Configuration Procedures	12-2
13-1 User Profile Configuration Procedures	13-1
13-2 File and Directory Permissions for the Profiles Folder	13-6
14-1 Default Computer Procedures	14-2

<b>Table</b>	<b>Page</b>
14-2 System Policy Editor - User Groups	14-10
14-3 Domain Users Properties	14-11
14-4 Privileged Users Properties	14-19
14-5 Domain Admins Properties	14-22
14-6 Finish With Policy Editor	14-25
15-1 Control Panel Configuration Procedures	15-1
17-1 System Repair Procedures	17-2
17-2 “Rdisk” Permissions	17-4
A-1 Hotfixes	A-1
B-1 Administrative Checklist	B-1

## Section 1

# Introduction

### 1.1 Purpose

Although Microsoft's Windows NT 4.0 (NT 4.0) operating system (OS) is still relatively new, NT 4.0 is gaining popularity worldwide as an inexpensive and user-friendly operating system for servers and workstations. In response to fleet demand, the Navy has issued formal record message traffic (R 300944Z MAR 97, INFORMATION TECHNOLOGY FOR THE 21ST CENTURY) directing the migration to Microsoft's Windows NT 4.0 Server and Workstation OS no later than December 1999.

Space and Naval Warfare Systems Command (SPAWAR) Information Security (INFOSEC) Program Office (PMW-161) has identified the need to provide clear and concise implementation guidance for NT 4.0 server and workstation installation. This guidance should be a step-by-step installation manual, with its primary focus on security configuration information.

### 1.2 Scope

This guide contains the installation and configuration procedures for securing the Microsoft Windows NT 4.0 operating system. The guide assumes that an installation is being made to a new computer or to one in which the previous installation is to be erased by formatting the hard drive. This installation is not to be performed as an upgrade from a previous version of an operating system, such as one of the following: Microsoft Disk Operating System (MS-DOS), 16-bit Windows (3.x, 3.11), OS/2, Windows 95, or Windows NT 3.x.

A Windows NT environment is composed of the following items: a workstation (the user's desktop), a server (file, print server), and a domain controller (primary and backup).

This document is intended to address the security concerns with the installation and implementation of the Microsoft Windows NT 4.0 operating system. It does not address prior versions of the NT operating system nor does it address the security concerns introduced by the installation of commercial off-the-shelf (COTS) or Government off-the-self (GOTS) applications. As time permits and by sponsor request, application installations may be included as appendices to the original document.

### 1.3 Background

Information superiority is the foundation of the Joint Vision 2010 battlefield dominance, as well as the war-fighting vision for each Service. Network warfare, robust infrastructure

and information dissemination to dispersed forces are key elements in achieving information superiority. Information Technology for the 21<sup>st</sup> Century (IT-21) is a fleet-driven reprioritization of command, control, communications, computers, and intelligence (C4I) programs of record to accelerate the transition to a PC-based tactical/tactical support war-fighting network. The inactivation of the current Department of Defense (DoD) messaging system (Automatic Digital Network [AUTODIN]) by December 1999, with no planned Navy infrastructure replacement, mandates the rapid implementation of this war-fighting network.

Commercial network operating systems (NOS) and e-mail products have achieved functional parity with each other. The fleets cannot continue to support a multitude of diverse operating systems and e-mail products with their own training, operational procedures, and troubleshooting requirements. The DoD Joint Technical Architecture (JTA) and Defense Information Infrastructure Common Operating Environment (DII COE) provide DoD with the automated information system (AIS) guidance required to take the Navy into the 21st Century. This convergence of solutions, problems, and guidance provides the impetus to establish minimum Navy AIS standards at this time. Implementation of this policy requires all non-standard NOS and e-mail products to be replaced no later than December 1999. The Microsoft Windows NT Server 4.0 is the standard fleet NOS. Windows NT 5.0 will soon follow. Windows NT Server 4.0 can be configured to be DII COE compliant.

Microsoft Exchange is designated as the standard e-mail solution for both fleets to ensure an interoperable secure messaging system is operational prior to AUTODIN inactivation no later than December 1999. Microsoft Office 97 is designated as the standard fleet office automation software. Hardware and software purchased today must be capable of meeting mission requirements through the year 2000.

Given the requirements above, SPAWAR PMW-161 believes it is necessary to guide the Navy in the secure implementation of the NT 4.0 deployment to the fleet. PMW-161 is working with Program Management Offices (PMOs) to understand their requirements and incorporate PMO OS requirements into a single NT 4.0 configuration and implementation guide. The results have been captured in this document.

## **1.4 Document Structure**

The *Secure Windows NT Installation and Configuration Guide* is designed to be used by Navy System Administrators during the installation of the OS in their environments. The basic document provides step-by-step instructions for the secure installation of NT 4.0 Server and Workstation. Section 1 provides an introduction to the document and project background. Section 2 lists system requirements and steps to be completed prior to installing the Windows NT 4.0 operating system. Section 3 lists step-by-step procedures for the blue screen installation of NT 4.0 server and workstation. Section 4 lists step-by-step procedures for the graphical installation of NT 4.0 server and workstation. Sections 3 and 4 cover the entire installation of NT 4.0 server and workstation from start to finish.

Section 5 begins the post-installation configuration portion of the document. This section covers the C2 Configuration Manager tool included in the Windows NT 4.0 Resource Kit for configuring your system to be C2-compliant. Section 6 lists procedures for securing the local file system, including shared files, directories, and executables. Section 7 provides instructions for setting up system audit policies and log files. Section 8 provides instructions for securing permissions and access to the Registry. Section 9 provides instructions for using the User Manager for Domains tool to create new groups and users and assign account restrictions. Section 10 provides instructions for configuring account policies, including password strength, logon hours, and user account expiration. Section 11 lists procedures to set up user rights policies for all users and groups in the domain. Section 12 lists instructions for configuring domain-wide policies, including adding and deleting trust relationships. Section 13 lists steps for configuring user profiles for new groups and users. Section 14 lists steps to secure the system policy for the entire domain. Section 15 lists steps for configuring various parts of the system through the Control Panel, including network protocols, services, desktop displays, printer setup, and general system information. Section 16 contains miscellaneous items to install or configure, such as password filters. Section 17 lists procedures for creating an Emergency Repair Disk and updating system repair data. The Bibliography contains Uniform Resource Locators (URLs) and cites books, manuals, and reports used. Appendix A lists hotfixes to download and install from Microsoft, and Appendix B lists actions that Administrators should perform on a regular basis to maintain the security of their domain. The Glossary lists acronyms contained in this guide.

## 1.5 Naming Conventions

The list below explains naming conventions used in this guide:

- **Angle braces.** Angle braces indicate the position in a text string where the generic description of the item described within the braces should be replaced with the proper name of the item specific to local conditions (e.g., if the NetBIOS name for your fileserver is PLATO, <fileserver> should be replaced by PLATO).
- **Double quotes.** Double quotes indicate text that should be entered exactly as it appears between the quotes, or the on-screen prompt/direction is repeated verbatim.
- **System variables.** System variables are referred through this document and take the form %<variable name>% (e.g., %systemroot%). These variables are intended to be used verbatim. It is not necessary to convert the environment variable to a local reference.
- **Hidden share names.** Hidden shares are identified by the share name follow by a \$ symbol (e.g., USERS\$). The \$ symbol must be entered as part of the share name to ensure the share is hidden.

## Section 2

# Pre-Installation

Pre-installation is the first of three phases of secure installation. This phase must be completed before beginning the second (blue screen non-graphical) and third phase (graphical), listed in Sections 3 and 4, respectively. The procedures included in this document apply to Intel-based PCs. Procedures for RISC-based systems (e.g., Alpha, PowerPC, MIPS) may vary. The following requirements must be met before beginning this process to ensure a smooth installation:

- **Physical security requirements.** Physical protections should include having a lockable central processing unit (CPU) box and placing the servers/controllers in a secured area.
- **Hardware requirements.** These installation procedures require a compact disk read-only memory (CD-ROM) drive and a 3.5-inch floppy drive. The processor should be a 486 or higher with 66 megahertz (MHz) minimum for both Windows NT workstations and servers. The CPU should have sufficient random access memory (RAM) (16 megabytes [MB] minimum, 64 MB recommended for a Windows NT workstation, and 16 MB minimum, 128 MB recommended for a Windows NT server) and sufficient disk space (110 MB minimum for the operating system, 2 gigabytes [GB] recommended for all disk partitions on a workstation, and 125 MB minimum for the operating system, 4 GB recommended for all disk partitions on a server).
- **Software requirements.** Software needed for this installation includes the Windows NT Server or Workstation 4.0 operating system (includes three floppy disks and a CD-ROM), the latest usable Service Pack (currently Service Pack 3 [SP3] with some hotfixes), and the Windows NT 4.0 Server and Workstation Resource Kits (three books and one CD-ROM for server, one book and one CD-ROM for workstation). SP3 can be found at the following URL:  
<ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/ussp3>.

In the first installation phase, back up all of the files currently on the computer to either a network share or a tape storage device. If only small portions of the hard drive will be needed later, back up those files to a floppy disk.

Certain system information needs to be obtained from the System Administrator prior to installing the Windows NT operating system. Table 2-1 lists information concerning hardware and software configuration that the user must specify during the installation process. This

information should be obtained from the System Administrator and written in the blank column below for later use during the actual installation.

**Table 2-1. System Configuration Information**

<b>Requested Installation Information</b>	
Network adapter card name and model number	
Graphic adapter name and model number	
Number of partitions on the hard drive (recommend two partitions: one 500 MB partition for the operating system, one 1500 MB partition for data and applications)	
IP address of the computer	
IP address of the Domain Name Service (DNS) server	
IP addresses of the primary and secondary Windows Internet Naming Service (WINS) servers	
IP address of the subnet mask	
IP address of the default gateway	
Name of the domain the workstations will join or servers will control	
Licensing method (per server or per seat)	
Computer name, up to 15 characters in length	

### Section 3

## Blue Screen Installation

Section 2 listed the first phase of Windows NT secure installation. In this second phase of installation, the user will be working with the three 3.5-inch floppy disks and the CD-ROM. The blue screens will present textual directions for the installation process. This portion of the installation is also known as the non-graphical phase, in contrast to the graphical phase identified in Section 4.

Table 3-1 lists the procedures for the blue screen installation for a Windows NT Workstation or Server. The Current Screen column describes the windows that appear on your monitor during the installation. The Procedure column lists the options throughout each step of the installation. The Rationale column explains the reasoning behind each procedure.

**Table 3-1. Blue Screen Installation Procedures**

	<b>Current Screen</b>	<b>Procedure</b>	<b>Rationale</b>
1.	Turned-off machine on which you will be installing Windows NT Workstation 4.0.	Boot the machine with Windows NT Workstation 4.0 using the first of three floppy disks entitled "Setup Boot Disk."	Begin the second phase of the secure installation procedure.
2.	The blue screen entitled "Windows NT Setup."	Insert the second floppy disk entitled "Setup Disk 2" when requested. Press ENTER.	Installation request.
3.	The blue screen entitled "Windows NT Workstation Setup," subtitled "Welcome to Setup."	Press ENTER to set up Windows NT Workstation 4.0.	Windows NT will begin installation at this time.

	<b>Current Screen</b>	<b>Procedure</b>	<b>Rationale</b>
4.	The blue screen entitled "Windows NT Workstation Setup."	Press ENTER to attempt to detect mass storage devices.	Allow Windows NT setup to attempt to detect mass storage devices.  Select Disk Controller Drivers.
5.	The blue screen entitled "Windows NT Workstation Setup."	Insert the third floppy disk entitled "Setup Disk 3" when requested.  Press ENTER.	Installation request.
6.	The blue screen entitled "Windows NT Workstation Setup."	Press ENTER.	NT setup should have found all mass storage devices.  Loading more device drivers.
7.	The blue screen entitled "Windows NT Workstation Setup."	Insert the "Windows NT Workstation" CD-ROM when requested.  Press ENTER.	Installation request.
8.	The blue screen entitled "Windows NT Licensing Agreement."	Read the licensing agreement.  Press Page Down several times.	Installation request.
9.	The blue screen entitled "Windows NT Licensing Agreement."	Press F8 to accept the licensing agreement.	You must accept the software license agreement to install the operating system.
10.	The blue screen entitled "Windows NT Workstation Setup."	Press enter to install a fresh copy of Windows NT.	Choose to perform a new installation.

	<b>Current Screen</b>	<b>Procedure</b>	<b>Rationale</b>
11.	The blue screen entitled “Windows NT Workstation Setup.”	Review the hardware and software components listed.  Highlight “The above matches my computer.”  Press ENTER.	Your computer software and hardware must be identified.
12.	The blue screen entitled “Windows NT Workstation Setup.”	Delete any existing partitions by pressing D. Press C to create a partition.	Split your drive into two partitions: the first for the operating system (500 MB) and the second for user data and applications (1500 MB for workstations or 3500 MB for servers).
13.	The blue screen entitled “Windows NT Workstation Setup.”	Press ENTER to create new partitions.	The reason for creating two partitions is ease of rebuilding the operating system and managing data for backups.
14.	The blue screen entitled “Windows NT Workstation Setup.”	Press ENTER to continue.	Accept the partition for the Windows NT operating system.
15.	The blue screen entitled “Windows NT Workstation Setup.”	Use the Down Arrow to highlight the NT File System (NTFS).  Press ENTER on the first partition.	NTFS provides security for directories and files.  All partitions must be NTFS formatted (including the system and the user data partitions). Section 5 (Table 5-1) includes instructions for formatting these partitions.  Do not format any partition using the FAT file system.

	<b>Current Screen</b>	<b>Procedure</b>	<b>Rationale</b>
16.	The blue screen entitled "Windows NT Workstation Setup."	Choose \WINNT as the location for NT files. Press ENTER.	This is the default location for the system directory where applications and utilities reside.
17.	The blue screen entitled "Windows NT Workstation Setup."	Press ENTER to perform an exhaustive secondary examination of hard disk(s).	The examination checks the integrity of the hard drive.
18.	The blue screen entitled "Windows NT Workstation Setup."	The blue screen phase portion of setup is completed. Remove any floppy disks and/or CDs. Press ENTER to restart your computer.	Setup files will be copied to the hard disk. The blue screen phase of setup is completed and the computer must be restarted.
19.	Startup screens as Windows NT reboots.	Wait for Insert Disk window.	Normal installation procedure.

## Section 4

# Graphical Window Installation

In this third phase of secure installation, the user will be working with the CD-ROM. The Windows NT Setup screens will present directions in graphical windows to continue the installation process. This portion of the installation is also known as the graphical phase, in contrast to the blue screen, non-graphical phase described in Section 3. If an error occurs during this phase, the user can return to the end of the blue screen phase and restart the installation from that point.

Table 4-1 lists the procedures for the graphical installation of a Windows NT Server. If you are installing a Windows NT Workstation, follow the procedures listed in Table 4-2. There are several steps in this guide that require the creation of the Emergency Repair Disk (ERD). The ERDs preserve configuration information throughout the installation process and provide a fallback position in the event of a system failure. While the timing of the ERD creation is a local issue, it is strongly recommended that at a minimum, System Administrators create an ERD at the end of the secure configuration (Section 17).

Table 4-1 consists of the following four phases: Information Gathering (13 steps), Network Setup (24 steps), Final Setup (10 steps), and First Logon (4 steps). The Current Window column describes the windows that appear on your monitor during the installation. The Procedure column lists the options throughout each step of the installation. The Rationale column explains the reasoning behind each procedure.

**Table 4-1. Graphical Window Installation Procedures for NT Server**

	<b>Current Window</b>	<b>Procedure</b>	<b>Rationale</b>
INFORMATION GATHERING			
1.	Insert Disk window.	Insert the CD labeled Windows NT Server 4.0. Click OK.	Installation request.
2.	Windows NT Server Setup window.	Click Next.	Begin setup.
3.	Windows NT Server Setup window, Name and Organization.	Type your full name and organization. Click Next.	Enter identification information.

	<b>Current Window</b>	<b>Procedure</b>	<b>Rationale</b>
4.	Windows NT Server Setup window.	Enter the CD key obtained from the CD case or from your System Administrator.	A valid key must be entered to install the operating system.
5.	Windows NT Server Setup, Licensing Mode.	If licensing per server, type in the number of concurrent connections for which you are licensed.	Number of connections is needed for license verification.
6.	Windows NT Server Setup window, Computer Name.	Type the name of the computer, up to 15 characters (this should be the same name entered later for Transmission Control Protocol/Internet Protocol [TCP/IP]). Click Next.	Keep the name of the computer consistent throughout the installation. Specifying the computer name will be in accordance with naming guide/scheme (e.g., DDG57CPC002).
7.	Windows NT Server Setup, Server Type.	Check Primary Domain Controller (PDC) if you are installing the first server in the domain, or Backup Domain Controller (BDC) if the Primary Domain Controller is already installed. Click Next.	The Primary Domain Controller must be installed before any other domain servers. A Backup Domain Controller stores account and group information and replaces a PDC in the event of system failure.
8.	Windows NT Server Setup window, Administrator Account.	Type the Administrator's password (between 8 and 14 characters long). Click Next.	Choose a password that is hard to guess to increase computer security. For example, the password should be at least 8 characters and should contain numbers and special characters.

	<b>Current Window</b>	<b>Procedure</b>	<b>Rationale</b>
9.	Windows NT Server Setup window, Emergency Repair Disk.	Select Yes to create an ERD. Click Next.	The emergency repair disk is used for repairing the operating system after damage due to viruses or system failures.
10.	Windows NT Server Setup window, Select Components.	Select Accessories. Click Details.	View the accessories for the system.
11.	Windows NT Server Setup window, Accessories.	Ensure Screen Savers is checked. Click OK.	Screen savers are required.
12.	Windows NT Server Setup window, Select Components.	Ensure both Communications and Windows Messaging are not checked. Click Next.	Windows messaging is not needed for installation.
13.	Windows NT Server Setup window.	Click Next.	Begin network installation.
<b>NETWORK SETUP</b>			
14.	Windows NT Server Setup window.	Check "Wired to the network." Click Next.	The computer will be participating on a network through a network adapter.
15.	Windows NT Server Setup.	Uncheck the box. Click Next.	Do not install the Internet Information Server (IIS) Web server.
16.	Windows NT Server Setup window.	Click Start Search.	A network adapter must be identified.
17.	Windows NT Server Setup window.	Ensure the adapter listed under Network Adapters is correct. Click Next.	Windows NT Server will find the proper network adapter.

	<b>Current Window</b>	<b>Procedure</b>	<b>Rationale</b>
18.	Windows NT Server Setup window.	Select the TCP/IP Protocol.  Only select NWLink if Netware resources are available on your network.  Do not select the NetBEUI Protocol.  Click Next.	For security reasons, only the minimum number of protocols should be installed.
19.	Windows NT Server Setup window.	Click Next.	Lists services that will be installed.
20.	Windows NT Server Setup window.	Click Next.	Begin installing selected components.
21.	Adapter Card Setup window.	Click Continue.	Accept the Adapter card setup information.
22.	TCP/IP Setup window.	If your server belongs to a local area network (LAN) which requires the use of DHCP, click Yes and skip to step 33.  If your server belongs to a LAN which does NOT require the use of DHCP, click No and continue with step 23.	Some networks require all machines to have a static IP address, while others require that all machines use dynamic IP addresses through a DHCP server.  NOTE: The following are some security issues when attempting to use the DHCP protocol:  Possible spoofing of the DHCP server.  No direct link (not easily auditable) between the IP number and an NT node.

	<b>Current Window</b>	<b>Procedure</b>	<b>Rationale</b>
23.	Microsoft TCP/IP Properties window, IP Address tab.	Type the appropriate IP Address, Subnet Mask, and Default Gateway. Click Advanced.	Conditional on step 22.
24.	Advanced IP Addressing window.	Check previous entries made. Ensure Enable PPTP Filtering is not checked. Check Enable Security. Click Configure.	Conditional on step 22.

	<b>Current Window</b>	<b>Procedure</b>	<b>Rationale</b>
25.	<p>TCP/IP Security window. Click Permit Only for TCP, UDP, and IP Ports. Click Add.</p> <p>**** Warning - unless the exact ports and services needed for your applications are known, this step should be skipped or should follow a locally prepared and tested port listing.</p>	<p>(OPTIONAL)</p> <p>Add the following TCP and UDP port numbers:</p> <p>20 (FTP data) *</p> <p>21 (FTP) *</p> <p>22 (SSH) SSH Remote Login Protocol</p> <p>23 (telnet)</p> <p>25 (smtp)</p> <p>53 (DNS)</p> <p>67 (DHCP/BOOTP Protocol Server) **</p> <p>68 (DHCP/BOOTP Protocol Server) **</p> <p>80 (HTTP)</p> <p>88 (Kerberos)</p> <p>90 (WINS)</p> <p>110 (POP3)</p> <p>137 (NetBIOS Name Service)</p> <p>138 (NetBIOS Datagram Service)</p> <p>139 (NetBIOS Session Service)</p> <p>161 (SNMP)</p> <p>162 (SNMPTRAP)</p> <p>443 (SSL)</p> <p>8080 (SHTTP)</p> <p>Add the following IP port numbers:</p> <p>6 (TCP)</p> <p>17 (UDP)</p> <p>Click OK.</p> <p>* Only needed if FTP service is installed.</p> <p>** Only needed if DHCP is being used.</p>	<p>Conditional on step 22.</p> <p>It is considered good security practice to tightly restrict system access and resources initially (e.g., shut down unused ports) and to ease these restrictions after deliberate study. This recommendation provides guidance in the form of a tightly restricted set of well-known ports to be enabled. All other ports will be blocked and not allow any inbound TCP/IP connections. Appropriately, it is a local decision to modify this list to meet operational policy/requirements. The complete list of well-known ports can be obtained from <a href="http://www.isi.edu/div7/iana">http://www.isi.edu/div7/iana</a>.</p> <p>NOTE: Ports 137 - 139 should be blocked on all routers and boundary machines with direct connections to the Internet (e.g., proxy servers). This prevents against certain attacks including RedButton and out-of-band data packets that can crash the system.</p>

	<b>Current Window</b>	<b>Procedure</b>	<b>Rationale</b>
26.	Advanced IP Address window.	Click OK.	Conditional on step 22. Advanced IP addressing complete.
27.	Microsoft TCP/IP Properties window, IP Address tab.	Click the DNS tab.	Conditional on step 22. Continue setting TCP/IP properties.
28.	Microsoft TCP/IP Properties window, DNS tab.	Type the appropriate Host Name (the Host Name typed should be the same as the Computer Name entered above in step 6) and Domain name. Click Add to type in the DNS Service Search Order and Domain Suffix Search Order.	Conditional on step 22. These values are required for DNS host name resolution. DNS is commonly used in most TCP/IP networks.
29.	Microsoft TCP/IP Properties window.	Click the WINS Address tab.	Conditional on step 22. Continue setting TCP/IP properties.
30.	Microsoft TCP/IP Properties window, WINS Address tab.	Type the appropriate IP addresses of the Primary WINS Server and Secondary WINS Server. Check "Enable DNS for Windows Resolution." Uncheck "Enable LMHosts Lookup." Leave the Scope ID field blank.	Conditional on step 22. The WINS service is required for Microsoft Networking to operate properly. Specifically, without WINS or an LMHOSTS file, a computer in a domain will not be able to locate the domain controllers to log in to the domain.
31.	Microsoft TCP/IP Properties window.	Click the Routing tab.	Conditional on step 22. Continue setting TCP/IP properties.

	<b>Current Window</b>	<b>Procedure</b>	<b>Rationale</b>
32.	Microsoft TCP/IP Properties window, Routing tab.	Ensure Enable IP Forwarding is not checked.	Conditional on step 22. All servers have a single network adapter and do not require IP forwarding.
33.	Microsoft TCP/IP Properties window, DHCP Relay tab.	Click the DHCP Relay tab if you are using DHCP instead of a static IP address for your machine. Click on the Add button and type in the IP address of the DHCP server in your network. Obtain the DHCP server's IP address from your System Administrator.  Click Apply and then click OK.	Conditional on step 22. The DHCP relay agent relays broadcast messages between the DHCP server and a client across an IP router.
34.	Windows NT Server Setup window.	Click Next.	Accept the network bindings listed.
35.	Windows NT Server Setup window.	Click Next.	Start the network to complete the installation of networking components.
36.	Windows NT Server Setup window.	Type the name of the valid domain that this computer will join.  If you are installing a BDC, enter the domain name and the username and password for the Domain Administrator.  Click Next.	Configures a machine to participate in the domain, or creates the domain if it does not yet exist.  The Domain Administrator account is needed to add the BDC to the specified domain.

	<b>Current Window</b>	<b>Procedure</b>	<b>Rationale</b>
37.	Windows NT Server Setup window.	Click Finish.	Finish setup configuration.
<b>FINAL SETUP</b>			
38.	Date/Time Properties window, Time Zone tab.	From the drop-down list, choose the correct time zone. Click Date & Time tab.	Set your proper time zone.
39.	Date/Time Properties window, Date & Time tab.	Enter the correct date and time. Click Close.	Set the correct date and time.
40.	Detected Display window.	Click OK.	Configure the display.
41.	Display Properties window.	Make changes as appropriate. Click Test.	Installation request.
42.	Testing Mode window.	Read text in the window. Click OK.	This test is required.
43.	Testing Mode window.	Click Yes or No as appropriate.	Installation request.
44.	Display Settings window.	Read text. Click OK.	Installation request.
45.	Display Properties window.	Check settings. Click OK.	Installation request.

	<b>Current Window</b>	<b>Procedure</b>	<b>Rationale</b>
46.	Setup window, Emergency Repair Disk. *** NOTE – An ERD will assist you in recovering to the recorded state. It is not necessary to make them throughout the installation process, but is imperative to make one at the conclusion and after any configuration modifications. All intermediate ERD's have been labeled OPTIONAL.	(OPTIONAL) Follow the directions on the screen.  Write the creation date on the ERD floppy disk.  Click OK.	The emergency repair disk is used for repairing the operating system after damage due to viruses or system failures.  It is recommended to create a new ERD immediately after the OS installation and after any configuration changes have been made to the system. This will provide a fallback position for each step of the configuration in the event of a system failure.
47.	Windows NT Setup.	Click on the graphical * button to restart the computer.	The computer must restart for the settings to take effect.
<b>FIRST LOGON</b>			
48.	Operating system option list.	You have 30 seconds to ensure the first entry (Windows NT Server version 4.00) is highlighted.  Press Enter.	Use the VGA mode option only when you are experiencing screen display problems.
49.	Begin Logon window.	Press Ctrl + Alt + Delete to log onto the machine.	Users should always press Ctrl + Alt + Delete for the secure logon screen provided by Windows NT.
50.	Logon Information window.	Type the password associated with the Administrator's account created earlier.	Logon session begins.

	<b>Current Window</b>	<b>Procedure</b>	<b>Rationale</b>
51.	Windows NT screen with Welcome window.	Read the information in the Welcome Screen.	Finished the secure installation procedure for Windows NT Server 4.0.

Table 4-2 lists the procedures for the graphical installation of a Windows NT Workstation. This table consists of the following four phases: Information Gathering (13 steps), Network Setup (22 steps), Final Setup (10 steps), and First Logon (4 steps). The Current Window column describes the windows that appear on your monitor during the installation. The Procedure column lists the options throughout each step of the installation. The Rationale column explains the reasoning behind each procedure.

**Table 4-2. Graphical Window Installation Procedures for NT Workstation**

	<b>Current Window</b>	<b>Procedure</b>	<b>Rationale</b>
<b>INFORMATION GATHERING</b>			
1.	Insert Disk window.	Insert the CD labeled "Windows NT Workstation 4.0." Click OK.	Installation request.
2.	Windows NT Workstation Setup window.	Click Next.	Installation request.
3.	Windows NT Workstation Setup window, Setup Options.	Accept the default setup option (Typical). Click Next.	Only advanced users should attempt a Custom setup. Choose the Portable or Compact option if necessary. NOTE: It is not needed to do a Custom installation in order to have the required security built in.

	<b>Current Window</b>	<b>Procedure</b>	<b>Rationale</b>
4.	Windows NT Workstation Setup window, Name and Organization.	Type your full name and organization. Click Next.	Enter identification information.
5.	Windows NT Workstation Setup window.	Enter the CD key obtained from the CD case or from your System Administrator.	A valid key must be entered to install the operating system.
6.	Windows NT Workstation Setup window, Computer Name.	Type the name of the computer, up to 15 characters (this should be the same name entered later for Transmission Control Protocol/Internet Protocol [TCP/IP]). Click Next.	Keep the name of the computer consistent throughout the installation.  Specifying the computer name will be in accordance with naming guide/scheme (e.g., DDG57CPC002).
7.	Windows NT Workstation Setup window, Administrator Account.	Type the Administrator's password (between 8 and 14 characters long). Click Next.	Choose a password that is hard to guess to increase computer security. For example, the password should be at least 8 characters and should contain numbers and special characters.
8.	Windows NT Workstation Setup window, Emergency Repair Disk (ERD).	Select Yes to create an ERD. Click Next.	The emergency repair disk is used for repairing the operating system after damage due to viruses or system failures.
9.	Windows NT Workstation Setup window, Windows NT Components.	Check "Show me the list of components so I can choose". Click Next.	A change in the required components is necessary.

	<b>Current Window</b>	<b>Procedure</b>	<b>Rationale</b>
10.	Windows NT Workstation Setup window, Select Components.	Select Accessories. Click Details.	View the accessories for the system.
11.	Windows NT Workstation Setup window, Accessories.	Ensure Screen Savers is checked. Click OK.	Screen savers are required.
12.	Windows NT Workstation Setup window, Select Components.	Ensure both Communications and Windows Messaging are not checked. Click Next.	Windows messaging is not needed for installation.
13.	Windows NT Workstation Setup window.	Click Next.	Begin network installation.
<b>NETWORK SETUP</b>			
14.	Windows NT Workstation Setup window.	Select "This computer will participate on a network." Check "Wired to the network." Click Next.	The computer will be participating on a network through a network adapter.
15.	Windows NT Workstation Setup window, adapters.	Click Start Search.	A network adapter must be identified.
16.	Windows NT Workstation Setup window, adapters.	Ensure that adapter listed under Network Adapters is correct. Click Next.	Windows NT Workstation will find the proper network adapter.

	<b>Current Window</b>	<b>Procedure</b>	<b>Rationale</b>
17.	Windows NT Workstation Setup window, network protocols.	Select the TCP/IP Protocol.  Only select NWLink if Netware resources are available on your network.  Do not select the NetBEUI Protocol.  Click Next.	For security reasons, only the minimum number of protocols should be installed.
18.	Windows NT Workstation Setup window, install networking components.	Click Next.	The networking components are ready to be installed.
19.	Adapter window.	Chose the proper adapter settings.  Click Continue.	The correct adapter must be chosen for proper system operation.
20.	TCP/IP Setup window.	If your workstation belongs to a LAN which requires the use of DHCP, click Yes and skip to step 32.  If your workstation belongs to a LAN which does NOT require the use of DHCP, click No and continue with step 21.	Refer to the above note on DHCP security issues in step 22 of Table 4-1.
21.	Windows NT Workstation Setup window.	Click Next.	Conditional on step 20.  Ready to start the network to complete the installation of networking components.

	<b>Current Window</b>	<b>Procedure</b>	<b>Rationale</b>
22.	Microsoft TCP/IP Properties window, IP Address tab.	Type the appropriate IP Address, Subnet Mask, and Default Gateway. Click Advanced.	Conditional on step 20. TCP/IP configuration.
23.	Advanced IP Addressing window.	Check previous entries made. Ensure Enable Point-to-Point Tunneling Protocol (PPTP) Filtering is not checked. Check Enable Security. Click Configure.	Conditional on step 20. Security settings.

	Current Window	Procedure	Rationale
24.	<p>TCP/IP Security window. Click Permit Only for TCP, UDP, and IP Ports. Click Add.</p> <p>**** Warning - unless the exact ports and services needed for your applications are known, this step should be skipped or should follow a locally prepared and tested port listing.</p>	<p>(OPTIONAL)</p> <p>Add the following TCP and UDP port numbers:</p> <p>67 (DHCP/BOOTP Protocol Server) **</p> <p>68 (DHCP/BOOTP Protocol Server) **</p> <p>80 (HTTP)</p> <p>88 (Kerberos)</p> <p>90 (WINS)</p> <p>137 (NetBIOS Name Service)</p> <p>138 (NetBIOS Datagram Service)</p> <p>139 (NetBIOS Session Service)</p> <p>161 (SNMP)</p> <p>443 (SSL)</p> <p>8080 (SHTTP)</p> <p>Add the following IP port numbers:</p> <p>6 (TCP)</p> <p>17 (UDP)</p> <p>Click OK.</p> <p>** Only needed if DHCP is being used.</p>	<p>Conditional on step 20.</p> <p>It is considered good security practice to tightly restrict system access and resources initially (e.g., shut down unused ports) and to ease these restrictions after deliberate study. This recommendation provides guidance in the form of a tightly restricted set of well-known ports to be enabled. All other ports will be blocked and not allow any inbound TCP/IP connections. Appropriately, it is a local decision to modify this list to meet operational policy/requirements. The complete list of well-known ports can be obtained from <a href="http://www.isi.edu/div7/iana">http://www.isi.edu/div7/iana</a>.</p> <p>NOTE: Ports 137 - 139 should be blocked on all routers and boundary machines with direct connections to the Internet (e.g., proxy servers). This prevents against certain attacks including RedButton and out-of-band data packets that can crash the system.</p>

	<b>Current Window</b>	<b>Procedure</b>	<b>Rationale</b>
25.	Back to the Advanced IP Address window.	Click OK.	Conditional on step 20. Advanced IP addressing completed.
26.	Microsoft TCP/IP Properties window, IP Address tab.	Click the DNS tab.	Conditional on step 20. Continue setting TCP/IP properties.
27.	Microsoft TCP/IP Properties window, DNS tab.	Type the appropriate Host Name (the Host Name typed should be the same as the Computer Name entered above in step 6) and Domain name. Click Add to type in the DNS Service Search Order and Domain Suffix Search Order.	Conditional on step 20. These values are required for DNS host name resolution. DNS is commonly used in most TCP/IP networks.
28.	Microsoft TCP/IP Properties window.	Click the WINS Address tab.	Conditional on step 20. Continue setting TCP/IP properties.
29.	Microsoft TCP/IP Properties window, WINS Address tab.	Type the appropriate Primary WINS Server and Secondary WINS Server.  Check "Enable DNS for Windows Resolution."  Uncheck "Enable LMHosts Lookup."  Leave the Scope ID field blank.	Conditional on step 20. The WINS service is required for Microsoft Networking to operate properly. Specifically, without WINS or an LMHOSTS file, a computer in a domain will not be able to locate the domain controllers to log in to the domain.
30.	Microsoft TCP/IP Properties window.	Click the Routing tab.	Conditional on step 20. Continue setting TCP/IP properties.

	<b>Current Window</b>	<b>Procedure</b>	<b>Rationale</b>
31.	Microsoft TCP/IP Properties window, Routing tab.	Ensure Enable IP Forwarding is not checked. Click Apply. Click OK.	Conditional on step 20. All workstations have a single network adapter and do not require IP forwarding.
32.	Windows NT Workstation Setup window, start the network.	Click Next.	Installation request.
33.	Windows NT Workstation Setup window.	Type the name of the valid domain that this computer will join. Check "Create a Computer Account in the Domain." Click Next.	Being a member of a domain is more secure than being a member of a workgroup since the security policy for a domain can be centrally administered.
34.	Create Computer Account in <domain name> window.	Enter the username and password of an account that has the ability to add workstations to the domain.	The domain computer account is needed to add the workstation to the specified domain.
35.	Windows NT Workstation Setup window.	Click Finish.	Finish setup configuration.
<b>FINAL SETUP</b>			
36.	Date/Time Properties window, Time Zone tab.	From the drop-down list, choose the correct time zone. Click Date & Time tab.	Set your proper time zone.
37.	Date/Time Properties window, Date & Time tab.	Enter the correct date and time. Click Close.	Set the correct date and time.

	<b>Current Window</b>	<b>Procedure</b>	<b>Rationale</b>
38.	Detected Display window.	Click OK.	Configure the display.
39.	Display Properties window.	Make changes as appropriate. Click Test.	Installation request.
40.	Testing Mode window.	Read text in the window. Click OK.	This test is required.
41.	Testing Mode window.	Click Yes or No as appropriate.	Finish testing mode.
42.	Display Settings window.	Read text. Click OK.	Installation request.
43.	Display Properties window.	Check settings. Click OK.	Installation request.
44.	Setup window, Emergency Repair Disk. *** NOTE – An ERD will assist you in recovering to the recorded state. It is not necessary to make them throughout the installation process, but is imperative to make one at the conclusion and after any configuration modifications. All intermediate ERD's have been labeled OPTIONAL.	(OPTIONAL) Follow the directions on the screen. Write the creation date on the ERD floppy disk. Click OK.	The emergency repair disk is used for repairing the operating system after damage due to viruses or system failures.  It is recommended to create a new ERD immediately after the OS installation and after any configuration changes have been made to the system. This will provide a fallback position for each step of the configuration in the event of a system failure.
45.	Windows NT Setup.	Click on the graphical * button to restart the computer.	The computer must restart for the settings to take effect.

	<b>Current Window</b>	<b>Procedure</b>	<b>Rationale</b>
<b>FIRST LOGON</b>			
46.	Operating system option list.	You have 30 seconds to ensure the first entry (Windows NT Workstation Version 4.00) is highlighted. Press Enter.	Use the VGA mode option only when you are experiencing screen display problems.
47.	Begin Logon window.	Press Ctrl + Alt + Delete to log onto the machine.	Users should always press Ctrl + Alt + Delete for the secure logon screen provided by Windows NT.
48.	Logon Information window.	Type the password associated with the Administrator's account created earlier.	Logon session begins.
49.	Windows NT screen with Welcome window.	Read the information in the Welcome Screen.	Finished the secure installation procedure for Windows NT Workstation 4.0.

## Section 5

# C2 Configuration Manager

The C2 Configuration Manager tool included with the Windows NT 4.0 Resource Kit enables a System Administrator to follow the ideals behind the C2 level of security and automate the steps needed to secure the Windows NT operating system. This section provides a step-by-step guide for using the C2 Configuration Manager.

## 5.1 Background

Security in Windows NT is based on guidelines developed by the U.S. Department of Defense (DoD). The C2 level of security included with Windows NT applies to standalone computers, not to network security. Network security is a different and much more complex security issue beyond the scope of this document.

C2 refers to a set of security policies that define how a secure system operates. The C2 evaluation process is separate from the C2 certification process. As of August 1995, the National Security Agency (NSA) granted the C2 security rating for Windows NT Server and Workstation version 3.5. As a result, these operating systems are on NSA's Evaluated Products List (EPL).

NOTE: This does not mean that Windows NT is C2 certified (no operating system is ever C2 certified). Certification applies to a particular installation, including hardware, software, and the system environment. It is up to an individual site to become C2 certified.

The requirements for A-, B-, C-, and D-level secure products are outlined in the *Department of Defense Trusted Computer System Evaluation Criteria* (TCSEC) published by the National Computer Security Center (NCSC). This publication is referred to as the "Orange Book," and is part of NSA's security "rainbow series." Security-level requirements are open to interpretations that change over time. When undergoing evaluation, each vendor negotiates with NSA about whether or not the details of its particular system implementation conform with the abstract security policy in NSA's books. The vendor must prove that the requirements have been met.

Microsoft has decided not to include certain components of NT in the evaluation process, not because they would fail the evaluation, but to save time by reducing the administrative workload on NSA. Additionally, the MS-DOS/Windows on Windows (WOW) system may be treated as a Win32 application and would therefore not need to be evaluated as part of the Trusted Computer Base (TCB). Networking on NT may not have to go through the "Red Book," or "Trusted Network Interpretation." It may be enough to consider networking to be another subsystem, and therefore only the Orange Book would apply. New or modified

components and other hardware platforms can go through a “RAMP” process to be included in the evaluation at a later time.

## **5.2 C2 Overview**

The security policy in C2 is known as Discretionary Access Control (DAC). In the Windows NT implementation, the basic concept is that users of the system:

- Own objects.
- Have control over the protection of the owned objects.
- Are accountable for all access-related actions.

C2 classification does not define a substantive security system in the sense of classified or unclassified data. (B-level security assumes the existence of an independent security classification system and enforces that system, but does not specify the substance of the classification system).

For example, in Windows NT, every object (e.g., file, Clipboard, window) has an owner; any owner can control other users’ access to its objects. The system tracks (audits) your actions for System Administrators (i.e., the System Administrator can track both successes and failures for accessed objects).

The key distinction between C-level and B-level security is access control. In a C2 (DAC) system, owners have absolute discretion about whether or not others have access to their objects. In a B-level, or Mandatory Access Control (MAC) system, objects have a security level defined independently from the owner’s discretion. For instance, if you receive a copy of an object marked “secret,” you cannot give permission to other users to see this object unless they have secret clearance. This is defined by the system independent of your discretion. MAC involves the concept of “data labeling,” which is the creation and maintenance by the system of security “labels” on data objects, unalterable by users (except in certain cases under system control and auditing). A System Administrator can obtain access to anyone’s objects, although it may require some programming (i.e., the user interface will not expose this right).

## **5.3 Preliminary Steps for C2 Configuration**

Some initial steps must be performed prior to running the C2 Configuration Manager. These steps include installing applications (e.g., Office, Internet Explorer), installing the latest Service Pack (SP3), resizing the Registry, installing hotfixes, creating an emergency repair disk (ERD), and installing the Windows NT 4.0 Resource Kit for server or workstation. All applications **MUST** be installed before the C2 Configuration Manager is run. The C2 tool makes changes to registry keys and file permissions which may prevent applications from being properly configured unless they are installed prior to running this tool. Once the applications, Service Pack, and hotfixes are installed, the System Administrator will then run

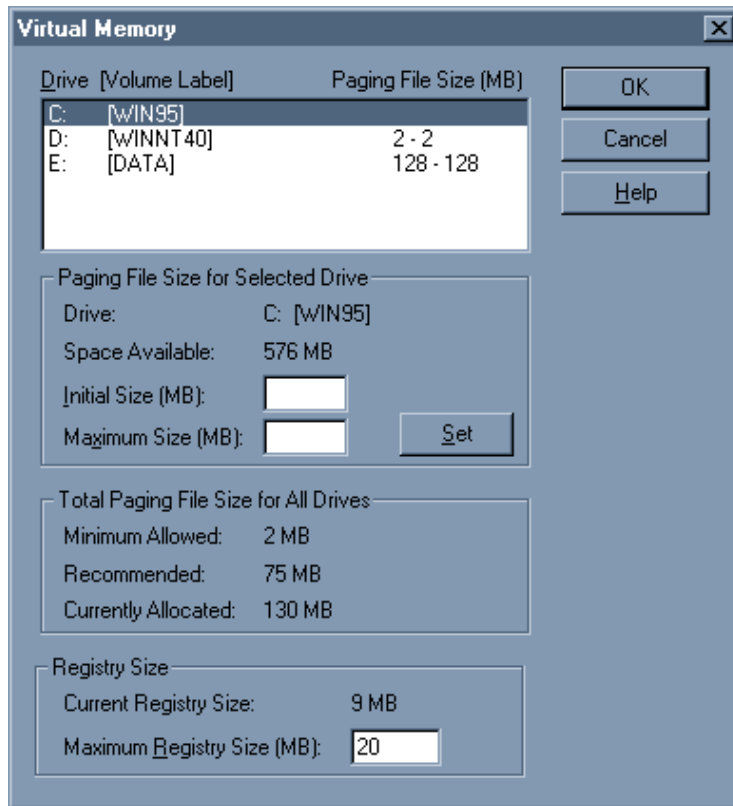
the C2 Configuration Manager tool and, when finished configuring the machine, create a new ERD.

Table 5-1 lists the steps to perform before starting the C2 Configuration Manager. These steps should be performed on all servers and workstations in the domain. The Navigate column lists the directions to view and open system windows. The Procedure column lists the options for each step of the configuration. The Rationale column explains the reasoning behind each procedure.

**Table 5-1. Pre-C2 Configuration Procedures**

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
1.	In the Taskbar, click on the Start button, Programs, and then Windows NT Explorer.	Right-click on the drive letter assigned to store data and applications (“D:”) and select Format.  In the Format D:\ window, select NTFS from the File System drop-down list. Click Start. Click OK in the warning window to format the drive.  Repeat for any other partitions created during the blue screen installation.	All partitions must be formatted to use the NTFS file system. (Refer to the discussion about NTFS formatting in step 15 of Table 3-1).
2.	Click on the Start button, Settings, and then Control Panel. Double-click on the Network icon and select the Services tab.	Verify that Peer Web Services is not present. If it is included in the list, highlight it and click on the Remove button.  Click OK. Close the Control Panel window.	Removes the Microsoft Peer Web Services which is used to run personal web servers on individual machines.
3.	The next two steps will create an emergency repair disk.  In the Taskbar, click on	When the Run window appears, type “rdisk /s” and then click the OK button.	Updates the system repair data with the latest configuration information.

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
	the Start button and then select Run.		
4.	When the rdisk utility finishes saving the current system information, a Setup window will appear.	(OPTIONAL) Click Yes to create the ERD. Insert a floppy disk labeled "ERD - Pre-Service Pack 3" and click OK.	Creates an updated copy of the ERD.
5.	Obtain Service Pack 3 from Microsoft. SP3 can be downloaded from the following URL: <a href="ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/ussp3">ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/ussp3</a>	Run the downloaded executable and follow the setup instructions on the screen to install SP3. Do not create an uninstall directory.	Service Pack 3 contains fixes to the Windows NT 4.0 server and workstation operating systems.
6.	After SP3 has successfully been installed, the registry size must be increased. In the Taskbar, click on the Start button, Settings, and then Control Panel. Double-click on the System icon and select the Performance tab.	Click on the Change button in the Virtual Memory area. When the Virtual Memory window appears (Figure 5-1), replace the "8" in the Maximum Registry Size (MB) box to "20." Click OK. Close the Control Panel window and do not restart the computer at this time.	Raises the registry size from 8 MB to 20 MB.



**Figure 5-1. Virtual Memory Window**

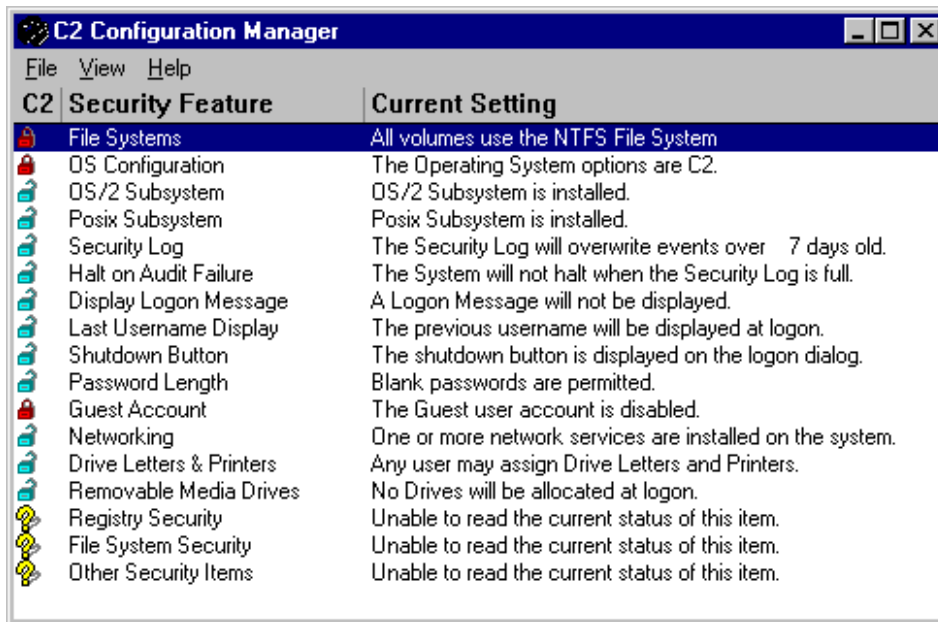
	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
8.	<p>Refer to Appendix A for a list and description of hotfixes to apply. Obtain the necessary post-SP3 hotfixes from Microsoft. These hotfixes can be downloaded from the following URL:</p> <p><a href="ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3">ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3</a></p>	<p>Download and install each hotfix in <b>ASCENDING ORDER</b> of their creation date.</p> <p>The machine will reboot after each hotfix has been successfully installed.</p>	<p>Hotfixes are executable programs that fix software bugs found in Windows NT server and workstation.</p>

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
9.	Another emergency repair disk must be created since the installations of SP3 and the post-SP3 hotfixes changed the system configuration.  In the Taskbar, click on the Start button and then select Run.	When the Run window appears, type “rdisk /s” and then click the OK button.	Updates the system repair data with the latest configuration information.
10.	When the rdisk utility finishes saving the current system information, a Setup window will appear.	(OPTIONAL)  Click Yes to create the ERD. Insert a floppy disk labeled “ERD - Post-Service Pack 3” and click OK.	Creates a new ERD with the latest system configuration information.
11.	The Windows NT 4.0 Resource Kit can now be installed.  Obtain the CD-ROMs containing the Resource Kit software.	Follow the setup instructions on the screen to install the Windows NT 4.0 Resource Kit.	After the Resource Kit is installed, the C2 Configuration Manager can be used.

## 5.4 Setting Up a C2-Compliant System

The C2 Configuration Manager lets you choose and implement the settings used in evaluating Windows NT for C2 security. For configuration details, use the on-line help utility included with the application.

To run the C2 Configuration Manager, click on the Start button, select Programs, Resource Kit 4.0, Configuration, and then C2 Config Manager. The main window (Figure 5-2) will display a summary of the security features that can be configured through the C2 Configuration Manager.



**Figure 5-2. C2 Configuration Manager Main Menu**

To modify the current setting of a security feature, highlight the desired item by using the mouse or the arrow keys, then double-click on the item or press the enter key.

For more detailed information on the selected item, press the F1 key or select Help from the menu.

The information in the main menu is listed under the following three columns:

- **C2.** This column provides a graphical indication of the current state-of-the-security feature. The icons used are explained below:
  - RED LOCK: Indicates the feature is configured to be C2 compliant.
  - BLUE LOCK: Indicates the feature is configured to be secure but is not required for C2 compliance.
  - OPENED BLUE LOCK: Indicates the feature has not been secured and is a possible security risk.
  - QUESTION MARK: Indicates the features could not be read by the C2 Configuration Manager.
- **Security Feature.** This column displays the name of the security feature.

- **Current Setting.** This column displays a short description of the current state of the security feature. For more detailed information on the selected item, press F1 for help.

Double-clicking on each security feature displays its configuration submenu. After completing the configuration for each item, a new emergency repair disk will need to be created. Do not overwrite the ERD created before the installation since it may be needed if an error is made while configuring the machine.

Each security feature in the C2 Configuration Manager's main menu is explained below. Complete the steps on every server and workstation in the domain to configure them for high-level security.

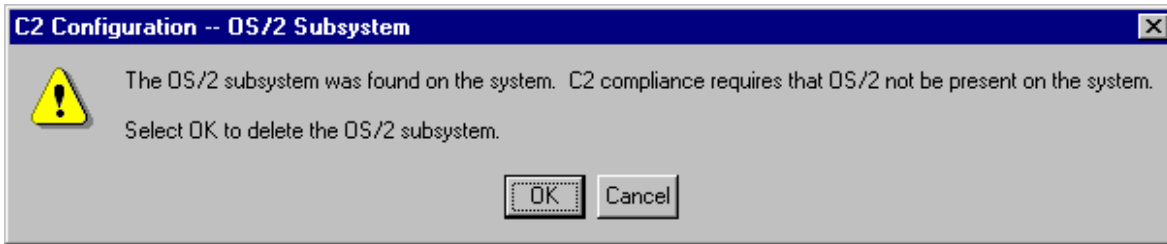
#### **5.4.1 File Systems and OS Configuration**

The first two features were already set on the machine used to create this guide. The file system on the machine's disk drive uses the NTFS file system and is reflected in the Current Setting column with a red lock in the C2 column.

The OS Configuration feature checks if the "boot.ini" file timer is set to zero, and ensures only the NT operating system is installed (not a dual-boot system). Double-click on OS Configuration to configure this feature. Since NT was the only operating system installed, the "C2 Configuration – OS Configuration" window reflects this fact. However, in order for an Administrator to boot to VGA mode in the event of a hardware problem, the "boot.ini" file timer must not be set to zero seconds. Refer to Section 6 for setting the timer for the "boot.ini" file. Click on the OK button. The system will return to the C2 Configuration Manager main menu, and the File System and OS Configuration Security features will have a blue lock in the C2 column.

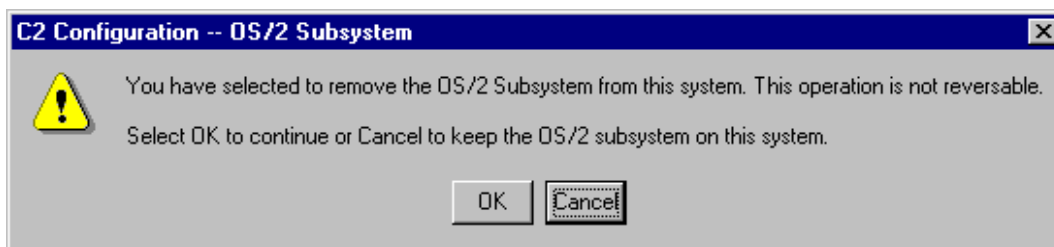
#### **5.4.2 OS/2 Subsystem Configuration**

Double-click on the OS/2 Subsystem feature to remove the OS/2 subsystem. The "C2 Configuration - OS/2 Subsystem" window (Figure 5-3) will appear.



**Figure 5-3. C2 Configuration - OS/2 Subsystem Window**

Click OK to remove this subsystem. The warning screen in Figure 5-4 will appear to confirm the removal.

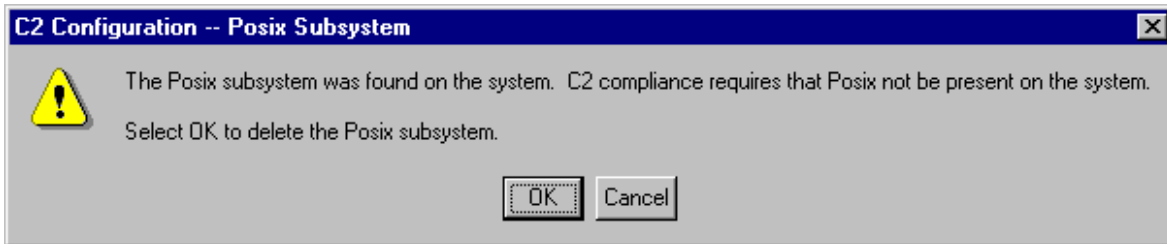


**Figure 5-4. C2 Configuration - OS/2 Subsystem Warning Window**

Click OK to remove the subsystem. The System Administrator will be returned to the C2 Configuration Manager main menu and the lock on the OS/2 Subsystem will be red.

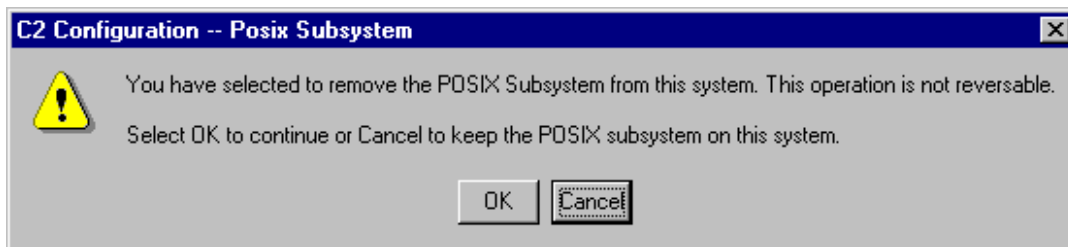
### **5.4.3 Posix Subsystem Configuration**

Double-click on the Posix Subsystem feature to remove the Posix subsystem. The “C2 Configuration - Posix Subsystem” window (Figure 5-5) will appear.



**Figure 5-5. C2 Configuration - Posix Subsystem Window**

Click OK to remove the subsystem. The warning screen in Figure 5-6 will appear.



**Figure 5-6. C2 Configuration – Posix Subsystem Warning Window**

Click OK to remove the subsystem. The System Administrator will be returned to the C2 Configuration Manager main menu and the lock on the Posix will be red.

#### **5.4.4 Security Log Configuration**

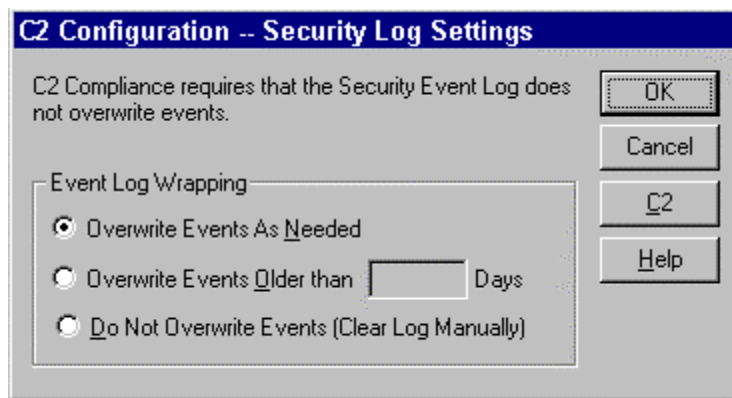
Double-click on the Security Log feature to display the Security Log Settings window (Figure 5-7). C2 configuration requires that the Security Event Log not be overwritten; however, this requires the System Administrator to manually clear the event logs periodically on each machine. For the Navy implementation, it is recommended that the setting be set to “Overwrite Events As Needed.” If the event log reaches its maximum size, new events will overwrite the oldest events. To ensure all audit data is recorded before being overwritten, the System Administrator must establish guidelines for archiving audit logs before the log reaches its maximum size.

The characteristics of the security log can be set in this window. The available options are:

- **Overwrite Events As Needed.** This option will overwrite the oldest events in the log once the log is full.

- **Overwrite Events Older than \_\_\_\_ Days.** This option will overwrite events that are older the specified age regardless of the size of the log.
- **Do Not Overwrite Events (Clear Log Manually).** This option will prevent the log from automatically destroying any logged events. The System Administrator must manually reset the log. This option must be selected for C2 compliance.

Select the “Overwrite Events As Needed” option (see Figure 5-7). Settings in this dialog box are made immediately after the OK button has been selected.

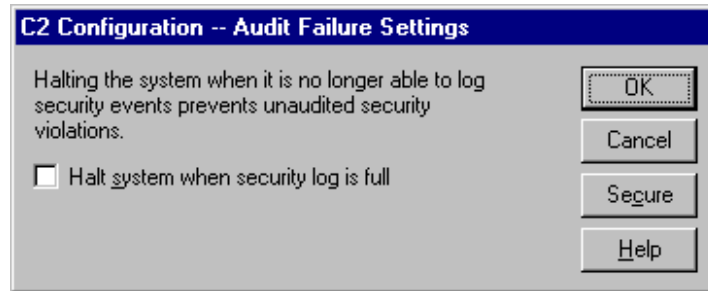


**Figure 5-7. C2 Configuration – Security Log Settings Window**

Click OK to accept this setting. The System Administrator will be returned to the C2 Configuration Manager main menu and the lock on the Security Log feature will be unlocked.

#### **5.4.5 Halt on Audit Failure**

If the security log becomes full, it is possible for some events to not be logged. Selecting the “Halt on Audit Failure” option will halt the computer when the log is full to prevent losing any events. If the system halts as a result of a full log, a System Administrator must restart the system and reset the log. DO NOT set this item. Double-clicking on the Halt on Audit Failure feature will display the window in Figure 5-8.



**Figure 5-8. C2 Configuration - Audit Failure Settings Window**

Press Cancel to continue and return to the C2 Configuration Manager main menu.

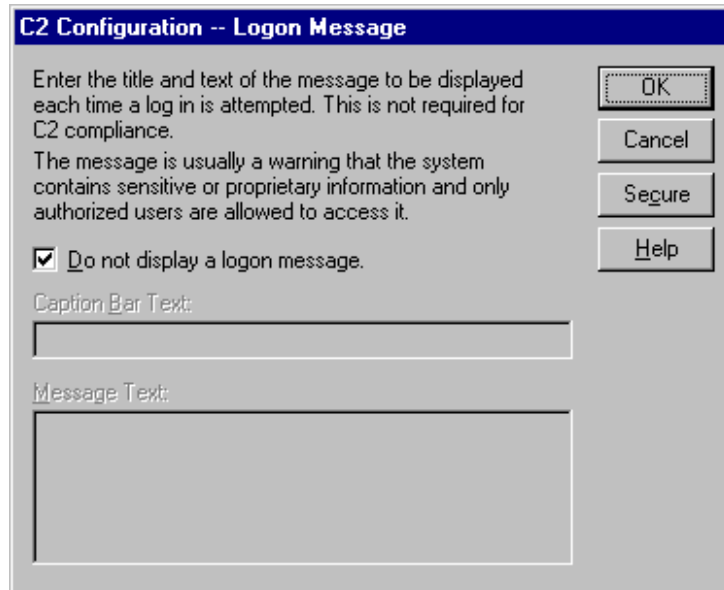
#### **5.4.6 Displaying a Legal Notice Before Log On**

This feature is used to create a logon message. The Navy 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) (<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:

“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.”

Windows NT displays a message box with a caption and text that can be configured before a user logs on to the machine. The Navy 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 onto the machine and browse the system.

Double-click on the Display Logon Banner feature in the C2 Configuration Manager main menu to display the Logon Message screen (Figure 5-9).



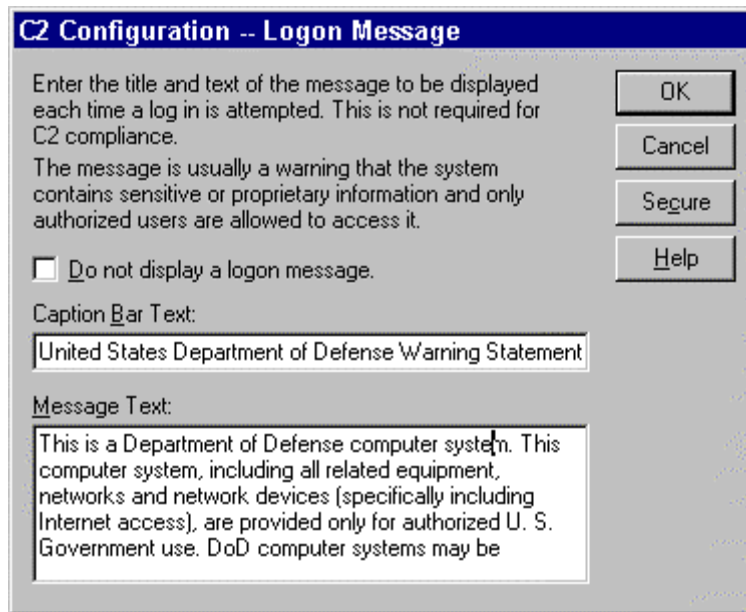
**Figure 5-9. C2 Configuration - Logon Message Window**

Clicking on the Secure button will display an alert (Figure 5-10).



**Figure 5-10. C2 Configuration - Logon Message Alert**

Click OK to return to the C2 Configuration - Logon Message window. Paste the text you copied from The United States Navy INFOSEC WebSite into the Message Text box and add the words “United States Department of Defense Warning Statement” to the Caption Bar Text box (see Figure 5-11).



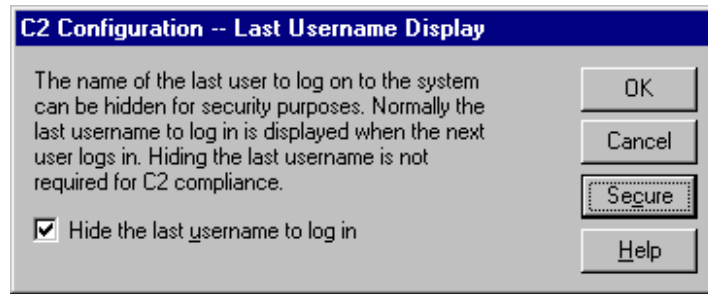
**Figure 5-11. C2 Configuration – Logon Message with Message Text**

Click OK to accept these changes. The System Administrator will be returned to the C2 Configuration Manager main menu and the lock on the Display Logon Message security feature will be blue. The Logon Message will be displayed the next time a person attempts to log on to the machine.

#### **5.4.7 Last Username Display**

Configure this feature to hide the last username on a machine.

By default, Windows NT places the username of the last user to log on the computer in the username text box of the Logon dialog box. This makes it more convenient for users to log on to the machine. However, displaying the name of the last user who was logged in to a machine provides a valid username to a potential hacker. To help keep usernames secret, prevent Windows NT from displaying the last username in the Logon dialog box. Double-clicking on the Last Username Display feature displays the window in Figure 5-12 with the “Hide the last username to log in” box unchecked.



**Figure 5-12. C2 Configuration – Last Username Display Window**

Click on the Secure button to hide the last username (the box will now be checked) and click OK. The System Administrator will be returned to the C2 Configuration Manager main menu and the lock on the Last Username Display security feature will be blue. The previous username will not be displayed the next time a person attempts to log on to the machine.

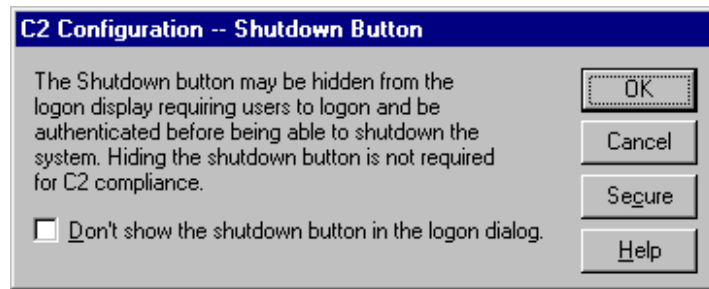
#### **5.4.8 Shutdown Button**

Normally, a user can shut down a computer running Windows NT without logging on by choosing Shutdown in the Logon dialog box. This is appropriate for users who can access the computer's operational switches; otherwise, they may tend to turn off the computer's power or reset the computer without properly shutting down the operating system. This feature can be removed if the CPU is physically protected and locked away.

Only valid users of a system should be able to shut down the machines. Otherwise, a non-user could force a reboot from a drive and bypass the security mechanisms.

The Navy's IT-21 implementation requires the shutdown button be displayed on the login display screen. If a System Administrator wishes to remove this button, the following steps should be performed.

Double-click on the Shutdown Button feature to display the dialog window shown in Figure 5-13.



**Figure 5-13. C2 Configuration - Shutdown Button Window**

Since the Navy's IT-21 implementation requires the shutdown button on the login screen, click on the cancel button. The System Administrator will be returned to the C2 Configuration Manager main menu and the lock on the Shutdown Button security feature will be unlocked.

#### **5.4.9 Password Length**

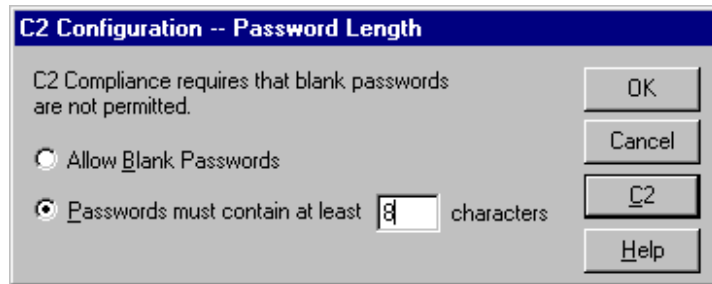
Blank passwords should never be allowed, and password lengths should be set to eight characters. Refer to Local Site Security Policy Guidance for specific password requirements. Users should take care to keep their passwords secret. Below are some tips for increasing password strength:

- Change passwords frequently and avoid reusing passwords.
- Avoid using easily guessed passwords such as:
  - Your name
  - Your spouse's name
  - Children's or pet's names
  - Any words that appear in the dictionary
  - Your UserID
- Do not write a password down.
- Choose a password that is easy for you to remember.
- Choose a password that contains a combination of letters, numbers, and special characters.

The minimum password length for all new passwords is specified in this window. The top radio button will allow blank passwords, while the bottom radio button will specify a minimum password length. Selecting the C2 button will require a minimum password length of six characters, however this value can be as small as one.

Double-clicking on the Password Length Security feature in the C2 Configuration Manager main menu displays the “C2 Configuration - Password Length” window (Figure 5-14).

Click on the radio button in front of “Password must contain at least \_\_\_\_ characters”, and then click in the box and type “8”. This will set the minimum password length to eight characters.



**Figure 5-14. C2 Configuration – Password Length Window**

Click OK to accept this setting. The System Administrator will be returned to the C2 Configuration Manager main menu and the lock on the Password Length security feature will be red.

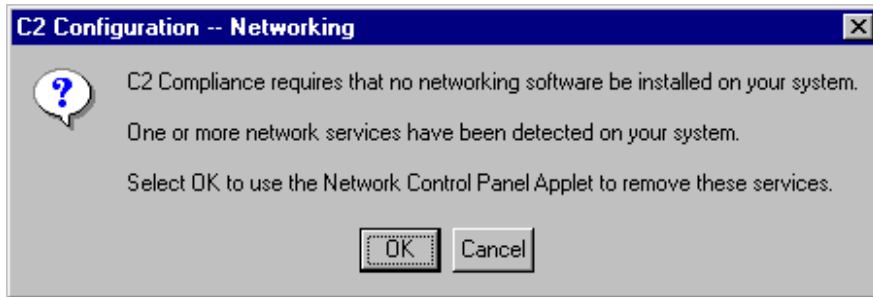
#### **5.4.10 Guest Account**

The Guest account allows anonymous (unauditable) access to a system and its files. C2-level security does not allow anonymous access to the system and therefore requires that Guest accounts be disabled or deleted.

The Guest account is disabled by default on all servers and workstations, therefore the lock should already be red in the C2 Configuration Manager main menu.

#### **5.4.11 Networking**

In order to set the C2 security requirements for the Networking feature, the machine must not use any networking software. Because the Navy’s IT-21 configuration requires machines be on an active network, this feature cannot be configured for C2 compliance. Enabling this feature prevents the use of the machine’s ethernet card. Double-clicking on the Networking Security feature displays the Networking window shown in Figure 5-15.

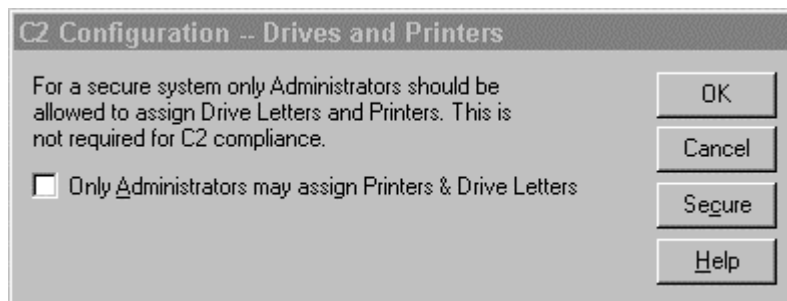


**Figure 5-15. C2 Configuration - Networking Window**

Press Cancel to continue. The lock next to the Networking feature will be unlocked in the C2 Configuration Manager main menu.

#### **5.4.12 Drive Letters and Printers**

To prevent redirection of data to an authorized device or port, the assignment of drive letters and printer ports can be restricted to System Administrators. Double-click on the Drive Letters & Printers feature to display the Drives and Printers window (Figure 5-16). Because the Navy's IT-21 configuration requires domain users to assign print drives, this feature cannot be configured for C2 compliance.



**Figure 5-16. C2 Configuration - Drivers and Printers Window**

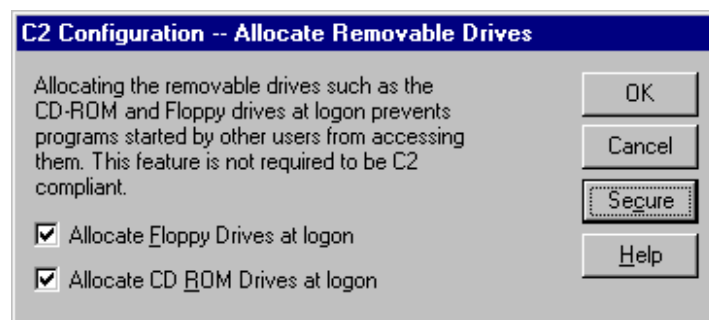
Click OK to accept this setting. The System Administrator will be returned to the C2 Configuration Manager main menu and the lock on the Drive Letters & Printers security feature will be unlocked.

### 5.4.13 Removable Media Drives

Since Windows NT is a multi-user system, programs executed by other users may run in the background while a user is logged on to a machine. Programs run on a machine by remote users can access disks in removable media drives that may have been inserted by a user physically using that machine. It is possible to prevent remote users from accessing these drives over the network.

Double-click on the Allocate Removable Drives feature. Select the Secure button to check both boxes and prohibit access to both the floppy and CD-ROM drives by programs run by other users (see Figure 5-17).

**WARNING:** It is not possible to share these drives when this feature is enabled. If you intend on sharing the floppy drive or CD-ROM drive over the network, the appropriate drive option must be unchecked. Changes made in this window are set immediately after the OK button has been selected, but will not take effect until the machine is restarted.

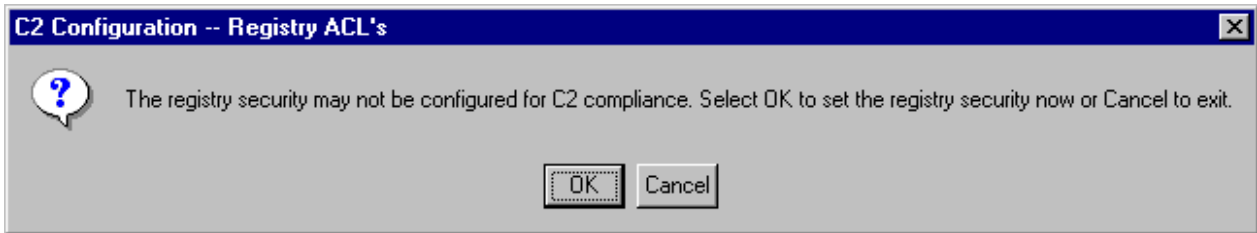


**Figure 5-17. C2 Configuration - Allocate Removable Drives Window**

Click OK to accept this setting. The System Administrator will be returned to the C2 Configuration Manager main menu and the lock on the Removable Media Drives security feature will be blue.

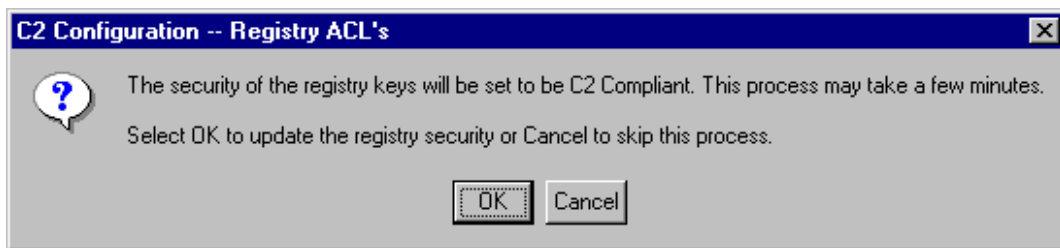
### 5.4.14 Registry Security

The Registry Security feature enables a System Administrator to assign ACLs that restrict access to the system registry keys. The permissions applied for C2 compliance are defined in the file "C2REGACL.INF." Double-click on the Registry Security feature to display the warning screen shown in Figure 5-18.



**Figure 5-18. C2 Configuration - Registry ACLs Warning Window**

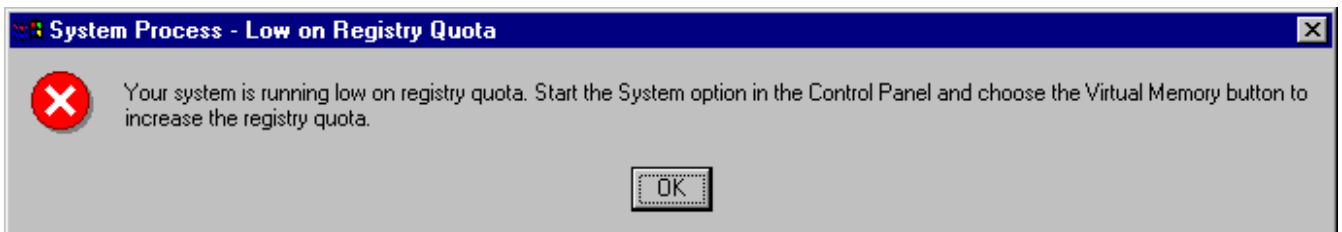
Click OK to set the registry security. The window in Figure 5-19 will be displayed.



**Figure 5-19. C2 Configuration - Registry ACLs Window**

Click OK and wait for the process to finish.

If you receive the following error (Figure 5-20), the registry size was not changed before starting the C2 Configuration Manager. This error will not effect the registry settings and is just a reminder to raise the quota. The registry must be resized when finished with the C2 Configuration Manager and after the machine has been rebooted.

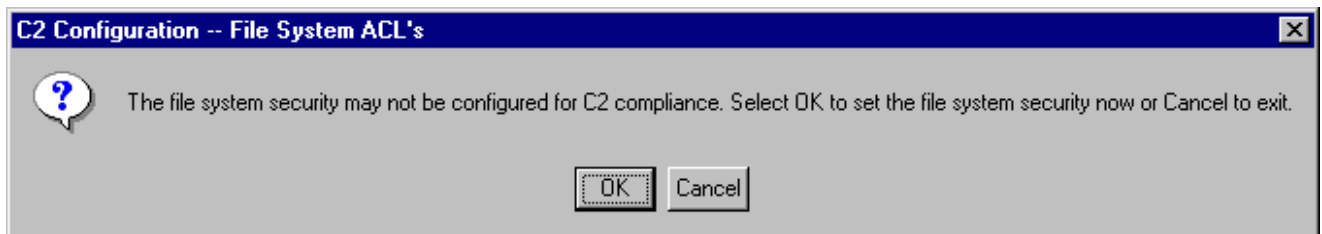


**Figure 5-20. Warning Message: System Process - Low on Registry Quota**

Click OK and wait for the process to complete. When the process is finished, the System Administrator will be returned to the C2 Configuration Manager main menu and the lock on the Registry security feature will be red.

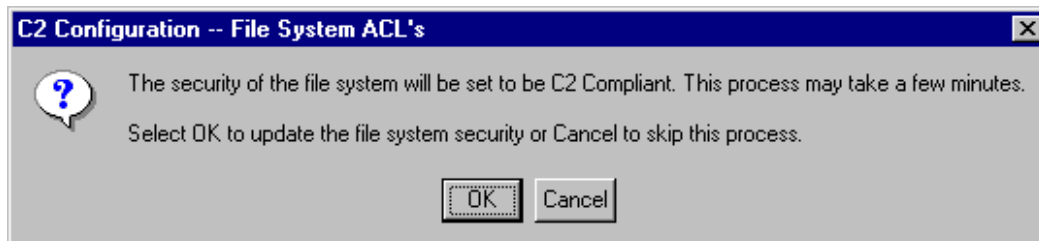
#### 5.4.15 File System Security

The File System security feature allows a System Administrator to assign ACLs for the files in the system folders. The permissions applied for C2 compliance are defined in the file “C2NTFACL.INF.” Double-click on the File System Security feature to display the warning screen shown in Figure 5-21.



**Figure 5-21. C2 Configuration - File System ACLs Warning Window**

Click OK to set the file system security. The screen in Figure 5-22 will be displayed.

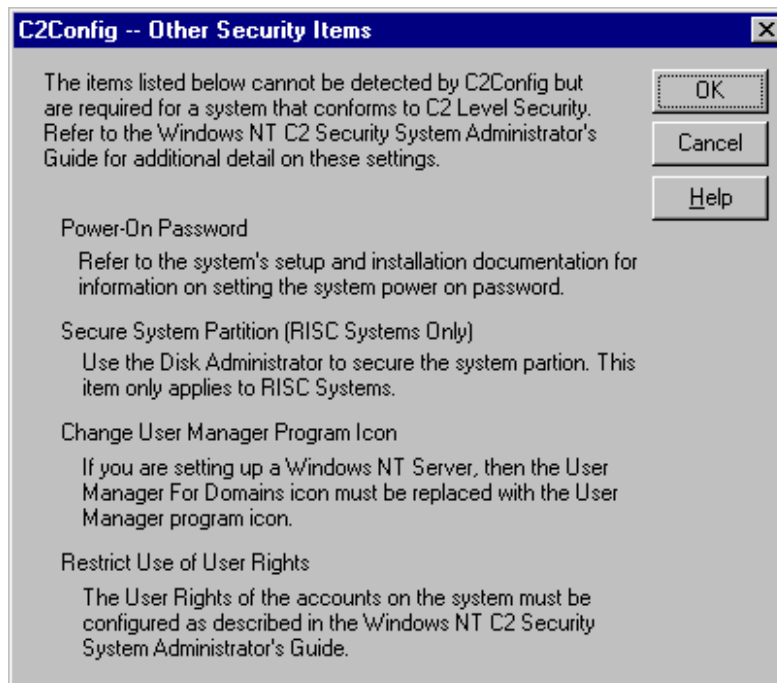


**Figure 5-22. C2 Configuration - File System ACLs**

Click OK and wait for the process to complete. When the process is finished, the System Administrator will be returned to the C2 Configuration Manager main menu and the lock on the File System security feature will be red.

### 5.4.16 Other Security Items

This is the final feature to configure using the C2 Configuration Manager. The C2 Configuration Manager is not able to detect or set all aspects of a Windows NT system in order to conform to C2-level security. Double-click on the Other Security Items security feature in the C2 Configuration Manager main menu. The C2 Configuration - Other Security Items window (Figure 5-23) will appear and explains additional information about configuring a C2 compliant system.



**Figure 5-23. C2 Configuration - Other Security Items Window**

The following list shows the items that are not detected and provides references to additional information about configuring these items:

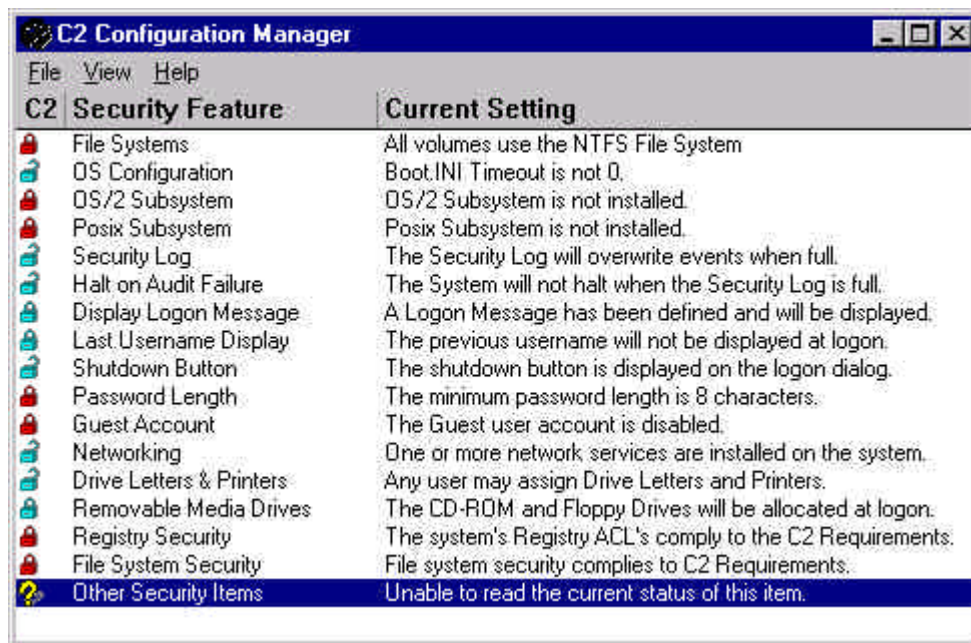
- **Power On Password.** The power on password requires the user to enter a password before the system starts. Refer to the computer systems documentation for information on setting this password.
- **Secure System Partition.** On a RISC computer, the Disk Administrator can be started and the Secure System Partition can be selected from the Partition Menu. This ensures that only users logged on as members of the Administrators group

can access files on the system partition.

Note: This is only required on RISC computers.

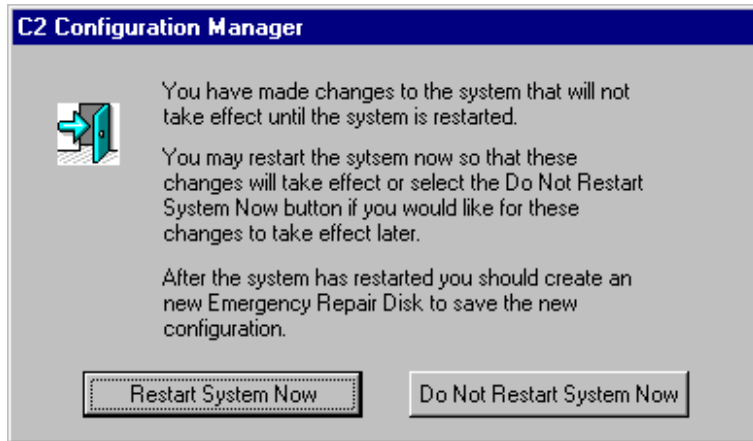
- **Change User Manager Program Icon.** On a Windows NT Server, the User Manager for Domains program can be removed and the User Manager program be added in its place as described in the Program Manager chapter of the Windows NT Workstation or Windows NT Server System Guide. The name of the executable file for User Manager is “MUSRMgr.EXE.”
- **Restrict Use of User Rights.** This is managed and configured by the User Manager program and is described in the User Manager chapter of the Windows NT Workstation or Windows NT Server System Guide. Rights should be limited as described in the Windows NT C2 Security System Administrators Guide.
- Clicking on the OK or Cancel button will return the System Administrator to the C2 Configuration Manager main menu.

The C2 Configuration Manager main menu should now look like Figure 5-24.



**Figure 5-24. C2 Configuration Manager Main Menu**

The machine will now need to be rebooted. Select File and then Exit from the menu bar. The window in Figure 5-25 will appear.



**Figure 5-25. C2 Configuration Manager Restart Message Window**

Select the “Restart System Now” button and wait for the system to reboot. When the machine has rebooted, a new ERD must be created since the system configuration has been changed by the C2 Configuration Manager. Refer to steps 2 and 3 in Table 5-1 for creating a new ERD, and label the new repair disk “ERD - Post C2 Config.”

## Section 6

# File System Configuration

Table 6-1 lists the default and allowable NTFS permissions for objects on Windows NT servers and workstations. The Object Types column lists objects on a file system. The Default Permissions column lists the permissions the operating system assigns by default to a new object. The Allowable Permissions column lists the possible permissions that can be assigned to any object in the file system.

**Table 6-1. Windows NT File and Directory Permissions**

<b>Object Type</b>	<b>Default Permissions</b>	<b>Allowable Permissions</b>
Files	Inherits permissions applied to the parent directory.	No Access – restricts all access Read – allows users to read and execute Change – allows users to read, write, execute and delete Full Control – same permissions as Change, but also includes right to create and modify NTFS file permissions and take ownership of NTFS files and folders Special Access – allows Administrators to customize permissions for a particular file (choose from read, write, execute, delete, change permissions, and take ownership)

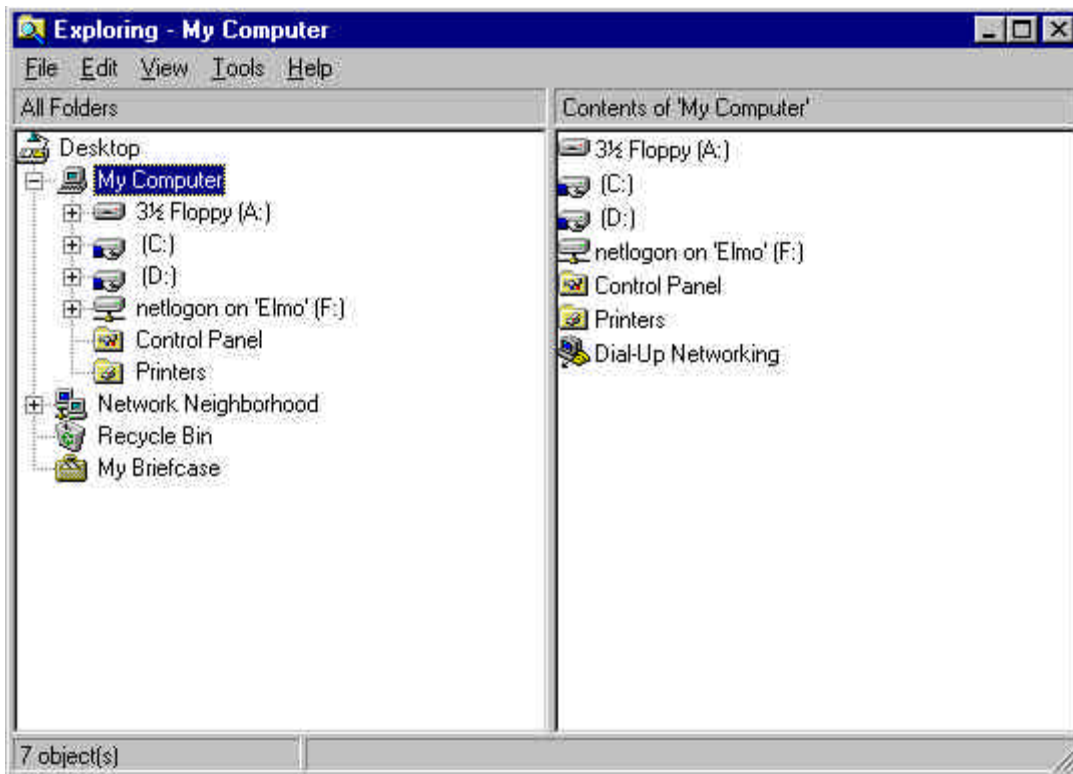
Object Type	Default Permissions	Allowable Permissions
Directories	Inherits permissions applied to the parent directory.	<p>No Access - restricts all access to the folder and its files</p> <p>List - allows users to view files and subfolders, but not access them</p> <p>Read - allows users to read and execute files</p> <p>Add &amp; Read - allows users to read, write, and execute files</p> <p>Change - allows users to create files, modify current files, and delete files and subfolders</p> <p>Full Control - same permissions as Change, but also includes right to create and modify NTFS file permissions and take ownership of NTFS files and folders</p> <p>Special Directory Access - allows Administrators to customize folder access permissions (choose from read, write, execute, delete, change permissions, and take ownership)</p> <p>Special File Access - allows Administrators to customize file access permissions (choose from read, write, execute, delete, change permissions, and take ownership)</p>

Object Type	Default Permissions	Allowable Permissions
Shares	<b>Everyone</b> Full Control	No Access - restricts all access to folders  Read - allows users to read and execute files  Change - allows users to create files, modify current files, and delete files and subfolders  Full Control - same permissions as Change, but also includes right to create and modify NTFS file permissions and take ownership of NTFS files and folders

Table 6-2 lists procedures for securing permissions on shared files, directories, and executables on the local file systems of servers and workstations. This table contains the following three sections: Network Shares, Directory Permissions, and File Permissions. The Navigate column lists the directions to view and open system windows. The Procedure column lists the options for each step of the configuration. The Rationale column explains the reasoning behind each procedure. By default, when changing directory permissions, the “Replace Permissions on Existing Files” option will be checked. Leave this option enabled unless otherwise specified in each step of the table.

**Table 6-2. File System Configuration Procedures**

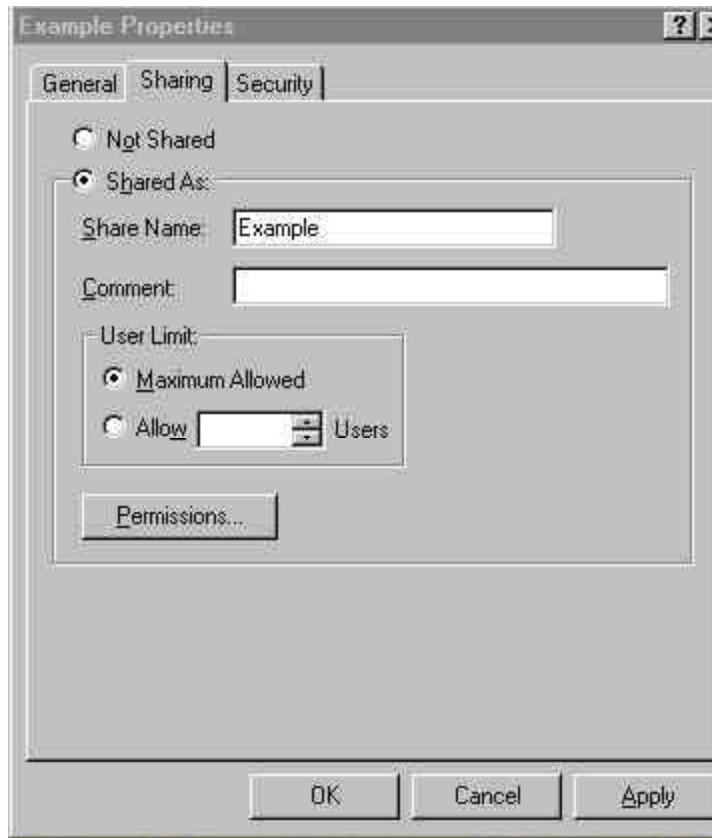
	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
<b>NETWORK SHARES</b>			
1.	<p>In the Taskbar, click on the Start button, select Programs, and then select Windows NT Explorer.</p> <p>When the Exploring window appears (Figure 6-1), right-click on the floppy drive, such as “3 ½ Floppy (A:)”, and then choose Properties.</p> <p>When the Properties window appears, select the Sharing tab.</p>	<p>Check the Not Shared option so that the floppy drive is not shared over the network.</p>	<p>Remote access to the floppy drive should be disabled to prevent another user from accessing the drive.</p>



**Figure 6-1. Windows NT Exploring Window**

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
2.	<p>In the Exploring window, right-click on the CD-ROM drive, such as “(E:)”, and then choose Properties.</p> <p>When the Properties window appears, select the Sharing tab.</p>	<p>Check the Not Shared option so that the CD-ROM is not shared over the network.</p>	<p>If the node is a CD-ROM server, then network access to the CD-ROMs is needed.</p> <p>Be careful to select only those CD-ROMs that are required to be on the network.</p>

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
3.	Click on one of the drives to display the list of folders contained on that drive. For all shares other than “C:\winnt” and individual drive letters, right-click on the shared folder (indicated by a hand under the folder) and select the Properties option. Click on the Sharing tab to display the share information about that folder (see Figure 6-2).	<p>Click on the Permissions button to display the Access Through Share Permissions window. By default, the group Everyone has Full Control to the share. Ensure permissions on all shared folders are set to:</p> <p><b>Authenticated Users</b> Read</p> <p><b>Administrators</b> Full Control</p> <p>Remove all other groups listed.</p> <p>These permissions allow only the Administrator to write and modify the shared folder while all users can read the contents.</p>	<p>The following default hidden shares are created for administrative purposes:</p> <p>ADMIN\$ C\$ IPC\$ NETLOGON</p> <p>These shares can not have their permissions changed, and are not visible to users browsing the network due to the dollar sign at the end of their name. Depending on their permissions, administrative shares can still be accessed by users who know their exact name by mapping a drive to the shared folder.</p> <p>Unauthorized users should not be allowed to modify or delete information contained in shared folders. Select users or groups can be given Change permissions to allow them to write and/or modify items in the folder.</p>



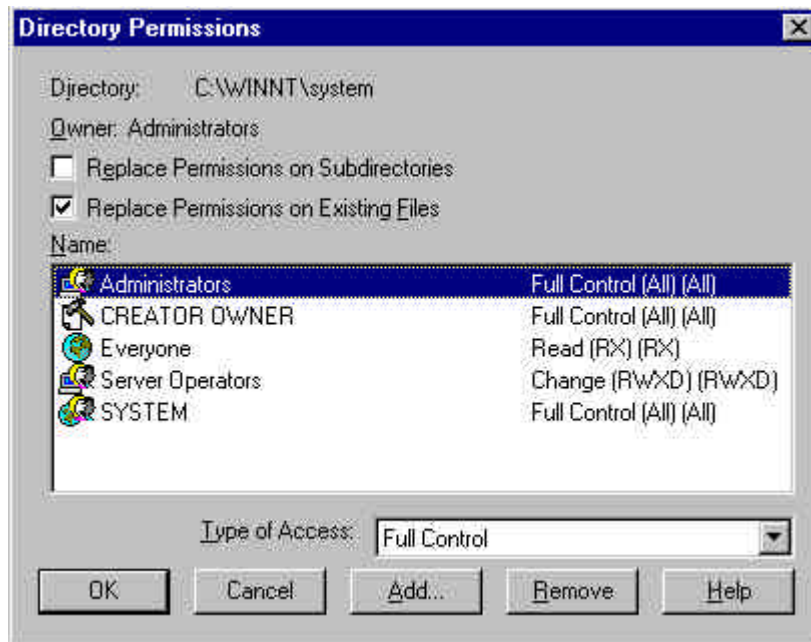
**Figure 6-2. Sharing Properties Window**

	Navigate	Procedure	Rationale
DIRECTORY PERMISSIONS			
4.	<p>In the Exploring window, right-click each TEMP or TMP directory listed, then select Properties.</p> <p>When the Properties dialog box appears, select the Security tab, then Permissions box.</p>	<p>Ensure permissions on all TEMP or TMP directories are set to:</p> <p><b>Administrators</b> Full Control</p> <p><b>CREATOR OWNER</b> Full Control</p> <p><b>Authenticated Users</b> Change</p> <p><b>SYSTEM</b> Full Control</p> <p>Click OK.</p>	<p>A temporary directory is one defined by the current environment variable "TEMP" or "TMP".</p> <p>These directories are used by many applications as a repository for temporary files containing data that should be protected from access by unauthorized users.</p>

	Navigate	Procedure	Rationale
5.	<p>In the Exploring window, right-click on a directory, such as “C:”, and then choose Properties.</p> <p>When the Properties window appears, select the Security tab, then Permissions.</p> <p>Verify the permissions on the directory.</p> <p>Repeat this procedure for other hard disk partitions, such as “D:”, etc.</p>	<p>Verify the permissions on each directory are set to:</p> <p><b>Administrators</b> Full Control</p> <p><b>CREATOR OWNER</b> Full Control</p> <p><b>Authenticated Users</b> Add and Read *</p> <p><b>Server Operators</b> ** Add and Read</p> <p><b>System</b> Full Control</p> <p>These permissions allow the group Everyone to create and add new files and directories, and by default, only the creator, “System”, or “Administrators” accounts will have access to the newly created files.</p> <p>Click OK. A warning box will appear since the “pagefile.sys” is in use by the operating system. Click Yes to continue.</p> <p>* For the system drive (“C:”) give Read access to the Everyone group instead of Add and Read.</p> <p>** Applies to DCs only.</p>	<p>These settings provide basic protection for each partition in the system.</p> <p>They also protect system files in the root directory, such as autoexec.bat, from being deleted and replaced with an attacker’s version.</p>

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
6.	<p>In the Exploring window, right-click on the “C:\Winnt” directory, and then choose Properties.</p> <p>When the Properties window appears, select the Security tab, then Permissions.</p>	<p>Verify the directory permissions are set to:</p> <p><b>Administrators</b> Full Control</p> <p><b>CREATOR OWNER</b> Full Control</p> <p><b>Authenticated Users</b> Add and Read</p> <p><b>SYSTEM</b> Full Control</p> <p>Ensure the groups Everyone and Users do not have Delete access.</p>	<p>These settings protect the operating system from unauthorized modification.</p> <p>With the use of these settings, only Administrators will be able to install most applications, and users of 16-bit applications may not be able to customize options.</p> <p>This is not as restrictive as is desirable, since it gives the Users group the Change access right to all “*.ini” files although this right may not be needed.</p> <p>Identifying which applications need the Change access right to their “.ini” files is difficult to do with complete accuracy.</p>

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
7.	<p>In the Exploring window, right-click on the “C:\Winnt\system” directory, then choose Properties.</p> <p>When the Properties window appears, select the Security tab, then Permissions (see Figure 6-3).</p>	<p>Verify the directory permissions are set to:</p> <p><b>Administrators</b> Full Control</p> <p><b>CREATOR OWNER</b> Full Control</p> <p><b>Authenticated Users</b> Read</p> <p><b>Server Operators *</b> Change</p> <p><b>SYSTEM</b> Full Control</p> <p>The groups Everyone and Users do not have Delete access.</p> <p>* Applies to DCs only.</p>	See above rationale.



**Figure 6-3. Directory Permissions Window**

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
8.	<p>In the Exploring window, right-click on the “C:\Winnt\system32” directory, then choose Properties.</p> <p>When the Properties window appears, select the Security tab, then Permissions.</p>	<p>Verify the permissions on this directory are set to:</p> <p><b>Administrators</b> Full Control</p> <p><b>CREATOR OWNER</b> Full Control</p> <p><b>Authenticated Users</b> Read</p> <p><b>Server Operators *</b> Change</p> <p><b>SYSTEM</b> Full Control</p> <p>* Applies to DCs only.</p>	<p>These settings protect the operating system from unauthorized modification.</p> <p>NOTE: To add new applications after these permissions have been applied, it may be necessary to change the Everyone group access to Change for proper installation. The permissions for Everyone should then be returned to Read once the application is installed.</p>
9.	<p>In the Exploring window, right-click on the “C:\Winnt\system32\drivers” directory, then choose Properties.</p> <p>When the Properties window appears, select the Security tab, then Permissions.</p>	<p>Verify the permissions on this directory on are set to:</p> <p><b>Administrators</b> Full Control</p> <p><b>CREATOR OWNER</b> Full Control</p> <p><b>Authenticated Users</b> Read</p> <p><b>Server Operators *</b> Full Control</p> <p><b>SYSTEM</b> Full Control</p> <p>* Applies to DCs only.</p>	<p>These settings are specified for C2 configuration and protect the operating system from unauthorized modification.</p>

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
10.	<p>In the Exploring window, right-click on the “C:\Winnt\system32\config” directory, then choose Properties.</p> <p>When the Properties window appears, select the Security tab, then Permissions.</p>	<p>Verify that the directory permissions are set to:</p> <p><b>Administrators</b> Full Control <b>SYSTEM</b> Full Control</p>	<p>The /config directory contains sensitive information, including the system’s event logs, and requires protection from unprivileged users.</p>
11.	<p>In the Exploring window, right-click on the “C:\Winnt\system32\spool” directory, then choose Properties.</p> <p>When the Properties window appears, select the Security tab, then Permissions.</p>	<p>Verify the permissions are set to:</p> <p><b>Administrators</b> Full Control <b>CREATOR OWNER</b> Full Control <b>Authenticated Users</b> Read <b>Print Operators *</b> Full Control <b>Power Users **</b> Change <b>Server Operators *</b> Full Control <b>SYSTEM</b> Full Control</p> <p>* Applies to DCs only. ** Applies to workstations only.</p>	<p>These settings are specified for C2 configuration.</p>
<b>FILE PERMISSIONS</b>			

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
12.	<p>In the Exploring window, click on Tools, Find, and then Files or Folders. In the Named field, type in “*.exe” and from the “Look in” drop-down list, select Local hard drives (C:, D:). Click on the Find Now button.</p> <p>Repeat for these files:</p> <ul style="list-style-type: none"> <li>*.bat</li> <li>*.com</li> <li>*.cmd</li> <li>*.dll</li> </ul>	<p>Select Edit and then Select All. Right-click on the highlighted list and select Properties.</p> <p>Verify the permissions on each file are set to:</p> <p><b>Administrators</b> Full Control</p> <p><b>SYSTEM</b> Full Control</p> <p><b>Authenticated Users</b> Read</p> <p>These settings will prevent any unauthorized modifications to executable programs. Modify file permissions according to the security officer or as needed.</p>	<p>These permissions protect operating system files and programs from being deleted or modified with an attacker’s version.</p>

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
13.	<p>In the Exploring window, select the “%systemroot%\system32” directory.</p> <p>NOTE: “C:\Winnt” is the default %systemroot% directory.</p>	<p>Restrict the following:</p> <p>Rcp.exe Rexec.exe Rpcss.exe Rsh.exe rdisk.exe ntbackup.exe regedit.* regedt32.*</p> <p>Right-click on each file, select Properties, select the Security tab in the Properties dialog box, and click on Permissions. Ensure the only permissions on each of these files are set to:</p> <p><b>Administrators</b> Full Control</p> <p><b>SYSTEM</b> Full Control</p> <p>Remove the Everyone group.</p>	<p>Regular users should not be able to execute these commands.</p>

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
14.	<p>In the Exploring window, click on View, Options, and select the “Show all files” option and uncheck the “Hide extensions for known file types” box. Click OK. Right-click on the “C:\boot.ini” file in the Exploring window and then choose Properties.</p> <p>When the Properties window appears, select the Security tab, then Permissions. Uncheck the “Read-only” attribute for the “boot.ini” file.</p> <p>Verify the file permissions.</p> <p>Repeat this procedure for files “C:\Ntndetect.com” and “C:\ntldr.”</p>	<p>Verify the permissions on each file are set to:</p> <p><b>Administrators</b> Full Control <b>SYSTEM</b> Full Control</p> <p>Remove the Everyone group.</p> <p>Double-click on the “boot.ini” file in the Exploring window to open the file in Notepad. Set the boot time-out to 3 seconds. Close the Notepad window. In the Exploring window, right-click on the “boot.ini” file, select Properties, and check the “Read-only” box. Click OK.</p>	<p>Setting the “boot.ini” file timer to 3 seconds allows Administrators to be able to boot the system to VGA mode.</p>

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
15.	<p>In the Exploring window, right-click on the “C:\Autoexec.bat” file, and then choose Properties.</p> <p>When the Properties window appears, select the Security tab, then Permissions.</p> <p>Verify the file permissions.</p> <p>Repeat this procedure for the “C:\Config.sys” file.</p>	<p>Verify the permissions on each file are set to:</p> <p><b>Administrators</b> Full Control</p> <p><b>Everyone</b> Read</p> <p><b>SYSTEM</b> Full Control</p>	<p>These settings are specified for C2 configuration on Intel platforms and protect the operating system from unauthorized modification.</p>
16.	<p>In the Exploring window, click on Tools, Find, and then Files or Folders. In the Named field, type in “*.ini” and from the “Look in” drop-down list, select Local hard drives (C:, D:). Click on the Find Now button.</p> <p>Do NOT change the permissions on the “boot.ini” file. It is important to keep the changes made in step 14 above.</p>	<p>Hold down the Control key and click on each file to select the entire list. Right-click on the highlighted list and select Properties.</p> <p>Reset the permissions on each file to:</p> <p><b>Administrators</b> Full Control</p> <p><b>Everyone</b> Read</p> <p><b>SYSTEM</b> Full Control</p> <p>The groups Everyone and Users do not have Delete access.</p>	<p>See above rationale.</p>

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
17.	<p>In the Exploring window, select the “%systemroot%\system32” directory. Right-click on each of the following files, then select Properties. In the Properties window, select the Version tab, then look at the text in the Description field.</p> <p>etexch32.dll  ntlmssps.dll   rsabase.dll  rsaenh.dll  schannel.dll  security.dll</p> <p>Repeat the same procedure for the following file in the “%systemroot%\system32\drivers” directory.</p> <p>ndiswan.sys</p>	<p>Ensure that each file’s version description information include any of the following text:  “US and Canada Use Only”,  “US/Canada Only”, or  “Domestic Use Only.”</p> <p>Check that each file’s version description information does not include the text “Export Version.”</p>	<p>This step is to check that the system only include 128-bit encryption. It is easy to load a new application (and even some hotfixes) and have the encryption regress to 40-bit. Also, installing the improper version of a service pack can decrease the encryption strength.</p>

**Section 7**

**Audit Policy Configuration**

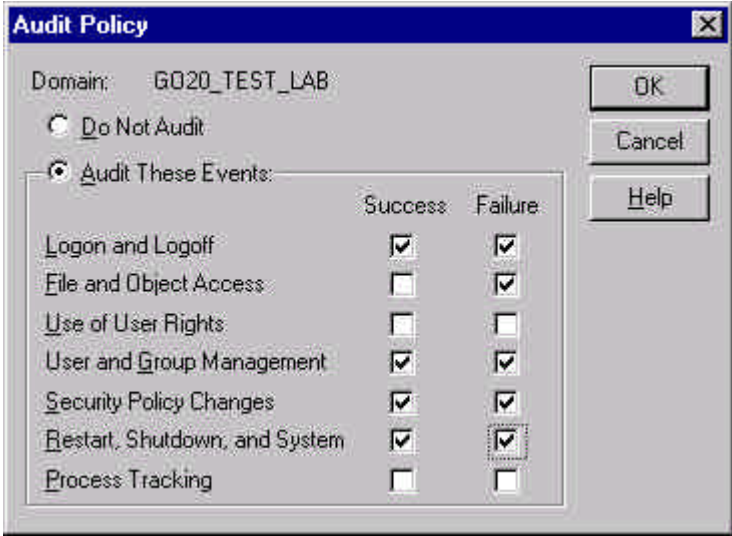
The auditing feature of Windows NT allows the Administrator to track who accesses or modifies files or directories. The audit log can be reviewed using the Event Viewer, which identifies potential security threats to your system.

Table 7-1 lists the steps to set up audit policies on your servers and workstations. The Navigate column lists the directions to view and open system windows. The Procedure column lists the options for each step of the configuration. The Rationale column explains the reasoning behind each procedure.

**Table 7-1. Audit Policy Configuration Procedures**

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
1.	To enable auditing on your machine, click on the Start button, Programs, Administrative Tools, and then choose User Manager for Domains (on servers) or User Manager (on workstations).	Choose Policies and then Audit. A window with the following options to audit on success or failure will appear (see Figure 7-1): Logon and Logoff File and Object Access Use of User Rights User and Group Management Security Policy Changes Restart, Shutdown, and System Process Tracking Select to audit on success and failure for Logon and Logoff, User and Group Management, Security Policy Changes, and Restart, Shutdown and System. Audit on failure	File and Object Access must be enabled to audit on directories/files and printers. Auditing on failed logins allows the System Administrator to check who is attempting to log into the system at different hours.  Auditing on successes for File and Object Access will fill the event logs rapidly and therefore should not be enabled.

	Navigate	Procedure	Rationale
		for File and Object Access.	



**Figure 7-1. Audit Policy Window**

	Navigate	Procedure	Rationale
2.	To audit on certain files, go to Windows Explorer and select the file you want to audit. Click on Tools, Find, and then Files or Folders. As an example, in the Named field, type in “*.exe” and from the “Look in” drop-down list, select Local hard drives (C:, D:). Click on the Find Now button.	Click on the Add button and select Everyone in the Name list box. Click Add and then OK.  Choose to audit failures for write and delete, and successes and failures for Change Permissions and Take Ownership.  Click OK twice.	At a minimum, audit “*.exe” in the “C:\Winnt” directory and all subdirectories.  You may want to select different events to audit depending on the particular files on your system. It is recommended to audit failed file deletions and modifications to keep track of file system

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
	In the Find window, click on Edit, then Select All to highlight the entire list. Right-click anywhere on the highlighted list and choose Properties. Click on the Security tab and then click Auditing. When asked to reset the security information on the selected items, click Yes.		integrity.
3.	To audit on certain directories, go to Windows Explorer and select the directory you want to audit. At a minimum, audit the “C:\Winnt\repair” and “C:\Winnt\system32\config” directories. Right-click on the folders one at a time and choose Properties. Click on the Security tab and then click Auditing.	Click on the Add button and select Everyone in the Name list box. Click Add and then OK.  Choose to audit failures for write and delete, and successes and failures for Change Permissions and Take Ownership.  Click OK twice.	Auditing these directories will monitor system repair data integrity and security information.
4.	To audit activity on registry keys, click on the Start button and then Run. Type “regedt32” in the Run Window to start the Registry Editor. In the editor window, select the key you want to audit. Click on Security in the menu bar	Check the Audit Permissions on Existing Subkeys box.  Click on the Add button to choose users and groups to audit. Once users and groups are added, you can select them in the Name list box and choose from the	If registry auditing is desired, it is recommended to audit success of key deletion and writing Discretionary Access Control (DAC) on a key.

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
	<p>and then Auditing. The Registry Key Auditing window will appear.</p> <p>It is not recommended to audit registry keys since the audit logs will be filled rapidly when registry auditing is enabled.</p>	<p>following events to audit on:</p> <p>Query Value</p> <p>Set Value</p> <p>Create Subkey</p> <p>Enumerate Subkey</p> <p>Notify</p> <p>Create Link</p> <p>Delete</p> <p>Write DAC</p> <p>Read Control</p> <p>Consult your System Administrator for setting auditing choices.</p>	
5.	<p>To change the settings of the audit logs, click on the Start button; then click on Programs, Administrative Tools, and Event Viewer. Click on Log in the menu bar and select Security log.</p> <p>Repeat for the Application and System logs.</p>	<p>Click on Log in the menu bar and choose log settings. The Event Log Settings Window will appear and you can set the maximum log size (in 64K increments) up to 4,194,240 kbytes. The recommended setting is 5056 kbytes.</p> <p>Refer to the Security Log Configuration portion of Section 5 to configure the log settings.</p>	<p>The size of each log should be configured based on the number of events and objects audited.</p> <p>Refer to page 5-10 in Section 5 for an explanation of the security log settings.</p>
6.	<p>In Windows Explorer, view the files in the “%systemroot%\system32\config” directory. The default security log file is named</p>	<p>Ensure that permissions are set to:</p> <p><b>Administrators</b> Full Control</p> <p><b>SYSTEM</b></p>	<p>Users other than the Administrator and System accounts should be denied access to the security log file.</p>

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
	“SecEvent.Evt.” Right click on this file and view the Properties.	Full Control  Remove all other groups.	

Table 7-2 lists procedures for archiving audit logs and securing permissions on a newly created directory for storing the archived logs. The Navigate column lists the directions to view and open system windows. The Procedure column lists the options for each step of the configuration. The Rationale column explains the reasoning behind each procedure.

**Table 7-2. Archiving and Securing Audit Logs**

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
1.	In the Taskbar, click on the Start button, Programs, and then select Windows NT Explorer. Traverse down the tree to the “C:\Winnt\system32” directory. Click on the “config” folder.	Select File, New, Folder from the File menu. Name the new folder “archives.”	Creates a directory to store archived event logs.
2.	Right-click on the “archives” folder and choose Properties. Click on the Security tab and then click on the Permissions button.	Ensure that the following permissions are set to:  <b>Administrators</b> Full Control  <b>CREATOR OWNER</b> Full Control  <b>SYSTEM</b> Full Control	Restricts access to the archives folder. If any other user or group is listed, remove them from the list.
3.	Click on the Start button, Programs, Administrative Tools (Common), and then	Select Application from the Log menu. Select “Save As” from the Log menu. Select the path as	Creates a copy of the Application log with a time sensitive name in a different directory.

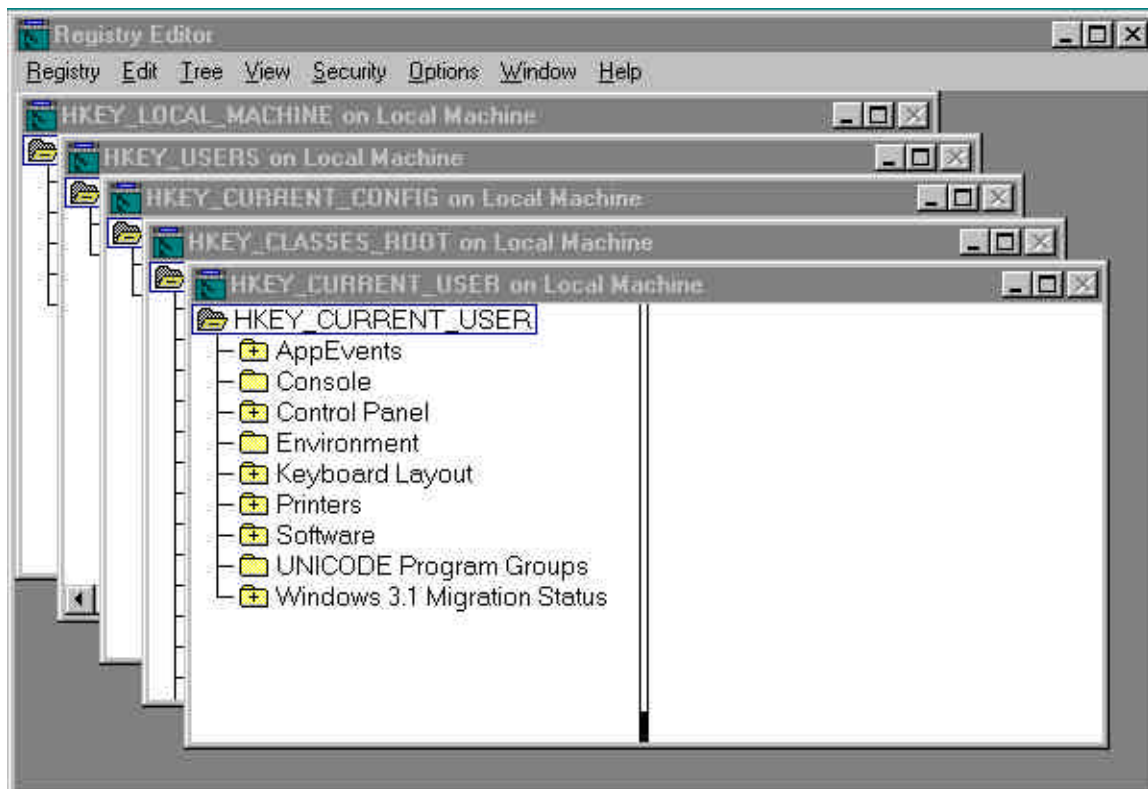
	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
	select Event Viewer.	“C:\Winnt\system32\config\archives.” Type a name in the name field that will reflect the log and its archive date (e.g., “app102197” for an application log archived on October 21, 1997). Click “Save.”	
4.	Repeat step 3 for the Security and System logs.	Name the new archived log files in a similar manner, but with a different prefix (e.g., “sec102197” or “sys102197”).	Archives the Security and System logs.

As an additional security measure, the archived event logs should be backed up, or permanently moved from the hard drive, to a data tape and physically secured.

## Section 8

# Registry Configuration

This section contains the registry configuration procedures, including actions that cannot be enabled from a graphical interface, such as the Control Panel, but must be performed on individual keys using the Registry Editor as shown in Figure 8-1. The procedures listed in Table 8-1 are individual actions that should be performed on every server and workstation to increase the security of the machines through the registry. These procedures have been grouped to simplify the task of securing a system. The Navigate column lists the directions to view and open system windows. The Procedure column lists the options for each step of the configuration. The Rationale column explains the reasoning behind each procedure.



**Figure 8-1. Registry Editor Window**

**Table 8-1. Registry Configuration Procedures**

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
1.	<p>In the Taskbar, click on the Start button, Programs, and then select Windows Explorer.</p> <p>When the Exploring window appears, select the “%systemroot%\system32” directory.</p> <p>Double-click on the “Regedt32.exe” file.</p>	<p>When the Registry Editor appears, click on the View menu, then select Tree and Data.</p>	<p>Bring up the Registry Editor once for use in this section.</p>
2.	<p>In HKEY_LOCAL_MACHINE, click on the Software Registry key, select the Security menu item, then Permissions.</p>	<p>When the Registry Key Permissions window appears, select Everyone in the Name box.</p> <p>In the Type of Access box, select the down arrow, choose Read, then click OK.</p> <p>Ensure the Network group privileges are None throughout the registry.</p> <p>Leave all other group permissions alone.</p>	<p>Removes the Everyone group from being able to install software.</p> <p>Prevents remote access over the network into the registry.</p>

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
3.	<p>In HKEY_LOCAL_MACHINE, double-click on the following registry key: Software\Classes</p> <p>Select the Security menu item and then Permissions.</p>	<p>When the Registry Key Permissions window appears, check the box Replace Permission on Existing Subkeys.</p> <p>Select Everyone and click Remove. Click on the Add button and select Authenticated Users in the Names box. Click OK. In the Type of Access list, select Special Access and check the following access rights:</p> <ul style="list-style-type: none"> <li>Query Value</li> <li>Set Value</li> <li>Create Subkey</li> <li>Enumerate Subkeys</li> <li>Notify</li> <li>Delete</li> <li>Read Control</li> </ul> <p>Click OK twice.</p>	<p>Restricts access to the actual file extension definitions to prevent changes to file associations and their associated applications.</p>

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
4.	<p>In HKEY_LOCAL_MACHINE, double-click on the following registry key: Software\Microsoft</p> <p>If installed, click on each of the following, select the Security menu item, and then Permissions.</p> <p style="padding-left: 40px;">ClipArt Gallery Shared Tools</p>	<p>When the Registry Key Permissions window appears, select Everyone and click Remove. Click on the Add button and select Authenticated Users in the Names box. Click Add.</p> <p>Check the box Replace Permission on Existing Subkeys.</p> <p>In the Type of Access box, select the down arrow, choose Full Control and then click OK.</p> <p>Repeat this procedure for the other subkey listed to the left.</p>	<p>Allows Full Control to the ClipArt Gallery and Shared Tools subkeys.</p>
5.	<p>In HKEY_LOCAL_MACHINE, double-click on the following registry key: Software\Microsoft\Rpc</p> <p>Select the Security menu item, and then Permissions.</p>	<p>Check the box Replace Permission on Existing Subkeys.</p> <p>Select Everyone in the Name box and click Remove.</p> <p>Click Add and select Authenticated Users. In the Type of Access box, select the down arrow, choose Read and then click OK twice.</p>	<p>Restricts access to the RPC services; prevents anonymous users from access to a remote node through RPC network services.</p>

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
6.	<p>In HKEY_LOCAL_MACHINE, double-click on the following registry key: Software\Microsoft\Windows\CurrentVersion</p> <p>Click on each of the following in turn, select the Security menu item, and then Permissions:</p> <p style="padding-left: 40px;">Run RunOnce Uninstall</p>	<p>When the Registry Key Permissions window appears, check the box Replace Permission on Existing Subkeys.</p> <p>Select Everyone in the Name box and click Remove.</p> <p>Click Add and select Authenticated Users. In the Type of Access box, select the down arrow, choose Read and then click OK.</p> <p>Repeat this procedure for the other subkeys listed to the left.</p>	<p>Prevents a valid local user or domain user from gaining Administrative rights or running programs that can cause damage.</p>
7.	<p>In HKEY_LOCAL_MACHINE, double-click on the following registry key: Software\Microsoft\Windows NT\CurrentVersion.</p> <p>Select the Security menu item and then Permissions.</p>	<p>When the Registry Key Permissions window appears, select Everyone and click Remove. Click on the Add button and select Authenticated Users in the Names box. Click Add.</p> <p>In the Type of Access box, select the down arrow, choose Read and then click OK.</p>	<p>Sets Read access to the specified key.</p>

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
8.	<p>In HKEY_LOCAL_MACHINE, double-click on the following registry key: Software\Microsoft\Windows NT\CurrentVersion</p> <p>Click on each of the following in turn, select the Security menu item, and then Permissions:</p> <ul style="list-style-type: none"> <li>AeDebug</li> <li>Compatibility</li> <li>Drivers32</li> <li>Embedding</li> <li>Fonts</li> <li>FontSubstitutes</li> <li>FontDrivers</li> <li>FontMapper</li> <li>FontCache</li> <li>GRE_Initialize</li> <li>MCI</li> <li>MCI Extensions</li> <li>ProfileList</li> <li>Type 1 Installer</li> </ul>	<p>When the Registry Key Permissions window appears, select Everyone and click Remove. Click on the Add button and select Authenticated Users in the Names box. Click Add.</p> <p>In the Type of Access box, select the down arrow, choose Read and then click OK.</p> <p>Repeat this procedure for each of the other subkeys listed to the left.</p>	<p>Sets Read access to the specified subkeys.</p>
9.	<p>At the same registry level, click PerfLib, select the Security menu item, and then Permissions.</p>	<p>When the Registry Key Permissions window appears, remove Everyone from the Name box.</p> <p>Click Add, select INTERACTIVE, and assign it Read access. Click OK.</p>	<p>Only allow local access to the system's performance data in addition to access for Administrators and System.</p>

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
10.	<p>In HKEY_LOCAL_MACHINE, double-click on the following registry key: Software\Microsoft\Windows NT\CurrentVersion</p> <p>Click on each of the following in turn, select the Security menu item, and then Permissions:</p> <p style="padding-left: 40px;">Ports Windows WOW</p>	<p>When the Registry Key Permissions window appears, select Everyone and click Remove. Click on the Add button and select Authenticated Users in the Names box. Click Add.</p> <p>In the Type of Access box, select the down arrow, choose Read and then click OK.</p> <p>Repeat this procedure for the other subkeys listed to the left.</p>	<p>Prevents a valid local user or domain user from gaining Administrative rights or running programs that can potentially cause damage.</p>
11.	<p>In HKEY_LOCAL_MACHINE, double-click on the following registry key: Software\Microsoft\Windows NT\CurrentVersion\Winlogon</p> <p>Select the Security menu item, and then Permissions.</p>	<p>When the Registry Key Permissions window appears, select Everyone and click Remove. Click on the Add button and select Authenticated Users in the Names box. Click Add.</p> <p>In the Type of Access box, select the down arrow, choose Read, then click OK.</p>	<p>Changing permissions from Special Access to Read removes the ability to write to the subkey. The default setting could allow a user to change the subkey and raise their access level to that of an Administrator.</p>

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
12.	In HKEY_LOCAL_MACHINE, double-click on the following registry key: Software\ Microsoft\Windows NT\CurrentVersion\ Winlogon	(OPTIONAL)  Select Edit from the Menu and then select Add Value.  When the Add Value window appears, type CachedLogonsCount in the Value Name box, select REG_SZ from the Data Type drop-down list, and then click OK.  When the String Editor dialog box appears, enter "0" and then click OK.	Prevents the caching of the last logon credentials for a user who logged on interactively to a system. This value entry specifies the number of credentials of previously logged on users that can be cached.
13.	In HKEY_LOCAL_MACHINE, double-click on the following registry key: Software\ Microsoft\Windows NT\CurrentVersion\ Winlogon	(OPTIONAL)  Select Edit from the Menu and then select Add Value.  When the Add Value window appears, type DeleteRoamingCache in the Value Name box, select REG_DWORD from the Data Type drop-down list, and then click OK.  When the String Editor dialog box appears, enter "1" and then click OK.	Prevents roaming profiles from being cached, limiting the amount of sensitive data on the system disk. This setting saves disk space, especially on workstations used by multiple people.

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
14.	<p>In HKEY_LOCAL_MACHINE, double-click on the following registry key: Software</p> <p>Click on Windows 3.1 Migration Status, select the Security menu item, and then Permissions.</p>	<p>When the Registry Key Permissions window appears, select Everyone and click Remove. Click on the Add button and select Authenticated Users in the Names box. Click Add.</p> <p>In the Type of Access box, select the down arrow, choose Read and then click OK.</p>	<p>Protects configuration data for the 16-bit environment.</p>
15.	<p>This step should be performed on DCs only. In HKEY_LOCAL_MACHINE, double-click on the following registry key: SYSTEM\ CurrentControlSet\ Services</p> <p>Click on Schedule, select the Security menu item, and then select Permissions.</p>	<p>When the Registry Key Permissions window appears, select Server Operators in the Name box.</p> <p>In the Type of Access box, select the down arrow, choose Read and then click OK.</p>	<p>Changing Server Operators permissions from Special Access to Read removes the ability to write to the subkey. The default setting could allow a member of the Server Operators group to change the subkey and raise their access to that of an Administrator.</p>

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
16.	<p>In HKEY_LOCAL_MACHINE, double-click on the following registry key: SYSTEM\ CurrentControlSet\ Services</p> <p>Click on UPS, select the Security menu item and then Permissions.</p>	<p>When the Registry Key Permissions window appears, select Everyone and click Remove. Click on the Add button and select Authenticated Users in the Names box. Click Add.</p> <p>In the Type of Access box, select the down arrow, choose Read and then click OK. Do not change permissions for any other groups listed.</p>	<p>Sets Read access to the specified subkeys.</p>
17.	<p>In HKEY_LOCAL_MACHINE, double-click on the following registry key: SYSTEM\ CurrentControlSet\ Services\LanmanServer</p> <p>Click on Shares, select the Security menu item, and then Permissions.</p> <p>On workstations only, repeat this step for the following registry key: SYSTEM\ CurrentControlSet\ Services\LanmanWorkstation</p>	<p>When the Registry Key Permissions window appears, select Everyone and click Remove. Click on the Add button and select Authenticated Users in the Names box. Click Add.</p> <p>In the Type of Access box, select the down arrow, choose Read and then click OK.</p>	<p>Protects the configuration of network shares and resources.</p>

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
18.	<p>In HKEY_LOCAL_MACHINE, double-click on the following registry key:  SYSTEM\  CurrentControlSet\  Services\LanmanServer\  Parameters</p>	<p>(OPTIONAL)</p> <p>Select Edit from the Menu and then select Add Value.</p> <p>On servers, when the Add Value window appears, type AutoShareServer in the Value Name box, choose REG_DWORD from the Data Type drop-down list, and then click OK.</p> <p>On workstations, when the Add Value window appears, type AutoShareWks in the Value Name box, choose REG_DWORD from the Data Type drop-down list, and then click OK.</p> <p>When the String Editor dialog box appears, enter "0" in the String box and then click OK.</p>	<p>This setting disables the creation of Administrative shares (e.g., C\$, D\$) at system boot time.</p>

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
19.	On servers only, in HKEY_LOCAL_MACHINE, double-click on the following registry key: SYSTEM\ CurrentControlSet\ Services\LanmanServer\ Parameters	(OPTIONAL)  Select Edit from the Menu and then select Add Value.  When the Add Value window appears, type EnableSecuritySignature in the Value Name box, choose REG_DWORD from the Data Type drop-down list, and then click OK.  When the String Editor dialog box appears, enter "1" in the String box and then click OK.	This settings enables signing into SMB packets from the server.  <b>WARNING:</b> Clients utilizing older dialects of the SMB protocol or for which packet signing is turned off may not be able to properly connect to a server with this setting turned on. Using SMB packet signing will slow down performance between 10 to 15 percent.
20.	In HKEY_LOCAL_MACHINE, double-click on the following registry key: SYSTEM\ CurrentControlSet\ Services\LanmanServer\ Parameters	Select Edit from the Menu and then select Add Value.  When the Add Value window appears, type RestrictNullSessAccess in the Value Name box, choose REG_DWORD from the Data Type drop-down list, and then click OK.  When the String Editor dialog box appears, type "TRUE" in the String box and then click OK.	Determines whether the Server service restricts access to clients using a null session. A null session is a session wherein the client is logged on to the system account without username and password authentication.  <b>True</b> Null session access is restricted  <b>False</b> Null session access is not restricted

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
21.	<p>In HKEY_LOCAL_MACHINE, double-click on the following registry key: SYSTEM\ CurrentControlSet\ Services\EventLog</p> <p>Click each of the following in turn: Application Security System</p>	<p>Select Edit from the Menu and then select Add Value.</p> <p>When the Add Value window appears, type RestrictGuestAccess in the Value Name box, choose REG_DWORD from the Data Type drop-down list, and then click OK.</p> <p>When the String Editor dialog box appears, enter “1” in the String box and then click OK.</p> <p>Repeat this procedure for the other subkeys listed to the left.</p>	<p>Only Administrators can access the event logs from the network.</p>
22.	<p>This step should be performed on workstations only. Skip this step if the workstations in the LAN are separated from the domain controllers by an internal router.</p> <p>In HKEY_LOCAL_MACHINE, double-click on the following registry key: SYSTEM\ CurrentControlSet\ Services\Browser\ Parameters</p>	<p>Select Edit from the Menu and then select Add Value.</p> <p>When the Add Value window appears, type MaintainServerList in the Value Name box, choose REG_SZ from the Data Type drop-down list, and then click OK.</p> <p>When the String Editor dialog box appears, type “no” in the String box and then click OK.</p>	<p>Stops workstations from maintaining a browser list for the Computer Browser service.</p> <p>If internal routers are placed between the domain controllers and workstations, the workstations need to maintain a browser list since the routers may not forward server broadcasts.</p>

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
23.	On workstations, in HKEY_LOCAL_MACHINE, double-click on the following registry key: SYSTEM\ CurrentControlSet\ Services\Rdr\Parameters	(OPTIONAL)  Select Edit from the Menu and then select Add Value.  When the Add Value window appears, type EnableSecuritySignature in the Value Name box, choose REG_DWORD from the Data Type drop-down list, and then click OK.  When the String Editor dialog box appears, enter "1" in the String box and then click OK.	Activates message signing into SMB packets from the workstation.  <b>WARNING:</b> Servers utilizing older dialects of the SMB protocol or for which packet signing is turned off may not be able to properly connect to a client which has packet signing enabled. Using SMB packet signing will slow down performance between 10 to 15 percent.
24.	In HKEY_LOCAL_MACHINE, double-click on the following registry key: SYSTEM\ CurrentControlSet\ Services\Rdr\Parameters	(OPTIONAL)  Select Edit from the Menu and then select Add Value.  When the Add Value window appears, type EnablePlainTextPassword in the Value Name box, choose REG_DWORD from the Data Type drop-down list, and then click OK.  When the String Editor dialog box appears, enter "0" in the String box and then click OK.	Prevents passing plain text (clear text) passwords  <b>WARNING:</b> Applications utilizing older dialects of the SMB protocol may not run properly with this setting enabled.

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
25.	In HKEY_LOCAL_MACHINE, double-click on the following registry key: SYSTEM\ CurrentControlSet\ Control\Lsa	<p>Select Edit from the Menu and then select Add Value.</p> <p>When the Add Value window appears, type Submit Control in the Value Name box, select REG_DWORD from the Data Type box, and then click OK.</p> <p>When the DWORD Editor dialog box appears, enter "1" in the Data box and then click OK. (Accept the default setting of "hex").</p>	<p>Allow System Operators to submit AT commands (scheduled tasks), in addition to Administrators.</p> <p><b>WARNING:</b> Running tools using the AT command will give those tools system privileges.</p>
26.	In HKEY_LOCAL_MACHINE, double-click on the following registry key: SYSTEM\ CurrentControlSet\ Control\Lsa	<p>(OPTIONAL)</p> <p>Only perform this step to audit base objects outside of files, registry keys, and printers.</p> <p>Select Edit from the Menu and then select Add Value.</p> <p>When the Add Value window appears, type AuditBaseObjects in the Value Name box, select REG_DWORD from the Data Type box, and then click OK.</p> <p>When the DWORD Editor dialog box appears, enter "1" in the Data box and then click OK.</p>	<p><b>WARNING:</b> Auditing all base objects will result in rapid growth of the audit logs. It is recommended to keep this option disabled.</p>

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
27.	In HKEY_LOCAL_MACHINE, double-click on the following registry key: SYSTEM\ CurrentControlSet\ Control\Lsa	(OPTIONAL)  Only perform this step to audit every privilege that is not audited by default.  Select Edit from the Menu and then select Add Value.  When the Add Value window appears, type FullPrivilegeAuditing in the Value Name box, select REG_BINARY from the Data Type box, and then click OK.  When the BINARY Editor dialog box appears, enter "1" in the Data box and then click OK.	Audits all user rights not audited by default, including Bypass Traverse Checking, Debug Programs, Create a Token Object, Replace Process Level Token, Generate Security Audits, Backup Files and Directories, and Restore Files and Directories.  WARNING: Auditing all privileges will result in rapid growth of the audit logs since the privileges above are frequent operations. It is recommended to keep this option disabled.
28.	In HKEY_LOCAL_MACHINE, double-click on the following registry key: SYSTEM\ CurrentControlSet\ Control\Lsa	Select Edit from the Menu and then select Add Value.  When the Add Value window appears, type CrashOnAuditFail in the Value Name box, select REG_DWORD from the Data Type box, and then click OK.  When the DWORD Editor dialog box appears, enter "0" in the Data box and then click OK.	Do NOT shut down the system when the audit logs become full.

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
29.	In HKEY_LOCAL_MACHINE, double-click on the following registry key: SYSTEM\ CurrentControlSet\ Control\Lsa	Select Edit from the Menu and then select Add Value.  When the Add Value window appears, type RestrictAnonymous in the Value Name box, select REG_DWORD from the Data Type box, and then click OK.  When the DWORD Editor dialog box appears, enter "1" in the Data box and then click OK.	This setting prevents anonymous connections from listing account names and enumerating share names. Anonymous connections from GUI management tools will receive an access denied error if they attempt to list account names.
30.	In HKEY_LOCAL_MACHINE, double-click on the following registry key: SYSTEM\ CurrentControlSet\ Control\Lsa	(OPTIONAL)  Select Edit from the Menu and then select Add Value.  When the Add Value window appears, type LMCompatibilityLevel in the Value Name box, select REG_DWORD from the Data Type box, and then click OK.  When the DWORD Editor dialog box appears, enter either "0", "1", or "2" (see Rationale in next column) in the Data box and then click OK.	This value controls the authentication type sent between machines:  <b>0</b> Send both Windows NT and LM password forms  <b>1</b> Send Windows NT and LM password forms only if the server requests it  <b>2</b> Never send LM password form  WARNING: If a Windows NT client select Level 2, it cannot connect to servers that support only LM authentication, such as servers based on Windows 95 and Windows for Workgroups.

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
31.	In HKEY_LOCAL_MACHINE, double-click on the following registry key: SYSTEM\ CurrentControlSet\ Control\Session Manager\Memory Management	Select Edit from the Menu and then select Add Value.  When the Add Value window appears, type ClearPageFileAt Shutdown in the Value Name box, select REG_DWORD from the Data Type box, and then click OK.  When the DWORD Editor dialog box appears, enter "1" in the Data box and then click OK.	This setting ensures the system page file will be cleared on a system shutdown so that any sensitive data stored in the page file will not be available to users.
32.	In HKEY_LOCAL_MACHINE, double-click on the following registry key: SYSTEM\ CurrentControlSet\ Control\ SecurePipeServers  Click on Winreg, select the Security menu item and then Permissions.  If the winreg key does not exist, click on SecurePipeServers, select Edit and then Add Key. Type "winreg" in the Key Name field and click OK.	When the Registry Key Permissions window appears, ensure that only Administrators with Full Control appears in the Name: box.  Remove all other groups listed.  Click OK.	Only Administrators can access the registry from the network.

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
33.	At the same Registry level, double-click on the Winreg registry key and then click on AllowedPaths.	<p>Ensure the entries in the Machine value are only the defaults created by a new installation of Windows NT:</p> <p>System\ CurrentControlSet\ Control\ProductOptions</p> <p>System\ CurrentControlSet\ Control\Print\Printers</p> <p>System\ CurrentControlSet\ Services\EventLog</p> <p>System\ CurrentControlSet\ Services\Replicator</p> <p>Software\Microsoft\ Windows NT\ CurrentVersion</p>	Do not add extra paths to the defaults listed.
34.	Click on HKEY_CLASSES_ROOT, select the Security menu item and then Permissions.	<p>When the Registry Key Permissions window appears, check the box Replace Permission on Existing Subkeys.</p> <p>Select Everyone and click Remove. Click on the Add button and select Authenticated Users in the Names box. Click Add.</p> <p>In the Type of Access box, select the down arrow, choose Read, and then click OK.</p>	Sets Read access to the specified subkeys.

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
35.	In HKEY_USERS, click on the .DEFAULT registry key, select the Security menu item and then Permissions.	When the Registry Key Permissions window appears, select Everyone and click Remove. Click on the Add button and select Authenticated Users in the Names box. Click Add.  In the Type of Access box, select the down arrow, choose Read, and then click OK.	Sets Read access to the specified subkeys.
36.	Verify that Access Control Lists (ACLs) on all registry keys used to support applications have been set to deny write and execute access for the group Everyone, but have granted the write and execute access for the Users group (on workstations and standalone servers) or the Domain Users group (on domain controllers).	This check should only be done if the Everyone group previously had write and execute access.	A utility such as DumpACL can be used to display the ACLs for the entire registry for easy viewing.  Even with the DumpACL utility, this task will be labor intensive.  DumpACL can be obtained from <a href="http://www.somarsoft.com/security.htm">http://www.somarsoft.com/security.htm</a>

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
37.	<p>This step should be performed on all machines running Microsoft Internet Explorer (IE) 3.02 (or earlier). By default, IE 3.02 does not register itself as an approved shell extension in the following registry key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Shell Extensions\ Approved</p> <p>Click on the Start button, Programs, and then Windows NT Explorer.</p>	<p>In the Exploring window, click on a directory (e.g., "C:\Temp") and select File, New, Text Document from the menu bar. Name the file "Enabie3.reg" and click Yes when prompted to rename the file. Right-click on this file and select Edit to open it in Notepad.</p> <p>Type in the following four lines:</p> <pre>REGEDIT4 [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Shell Extensions\ Approved] "{5E6AB780-7743-11CF-A12B-00AA004AE837}"= "Microsoft Internet Toolbar" "{3DC7A020-0ACD-11CF-A9BB-00AA004AE837}"= "The Internet"</pre> <p>Save the file, close the Notepad window, and then double-click on the file in the Exploring window. A message will appear indicating the information was entered into the registry.</p>	<p>When the "Only use approved shell extension" option is enabled (Section 14, System Policy Configuration) IE 3.02 will not run since it does not register itself as an approved extension when installed.</p> <p>Refer to article #Q166465 titled "Internet Explorer Does Not Start" in Microsoft's Knowledge Base (accessed at Microsoft's web site) for details on the "Enabie3.reg" file.</p>

## Section 9

# User Manager for Domains Configuration

The policy for an IT-21 environment is to place all user accounts at the domain level, with only the local built-in accounts (Administrator and disabled Guest accounts) placed on individual nodes. Domain-level accounts are located on a domain controller (either the primary or backup) with the User Manager for Domains being the administrative tool for creating and deleting groups and user accounts. By default, all users are members of the group Domain Users. Select users should also be added to a group with higher privileges to give them more administrative abilities. Consult with your System Administrator to identify these users.

The built-in Administrator's account should only be used once to build the minimum number of accounts requiring administrative privileges. All subsequent actions requiring administrative privileges (including the creation of regular user accounts) should use the individual accounts created with administrative rights. The reason for this is twofold: to protect the built-in Administrator's account since it cannot be locked out, and to provide accountability for the usage of privileged commands/rights/accounts.

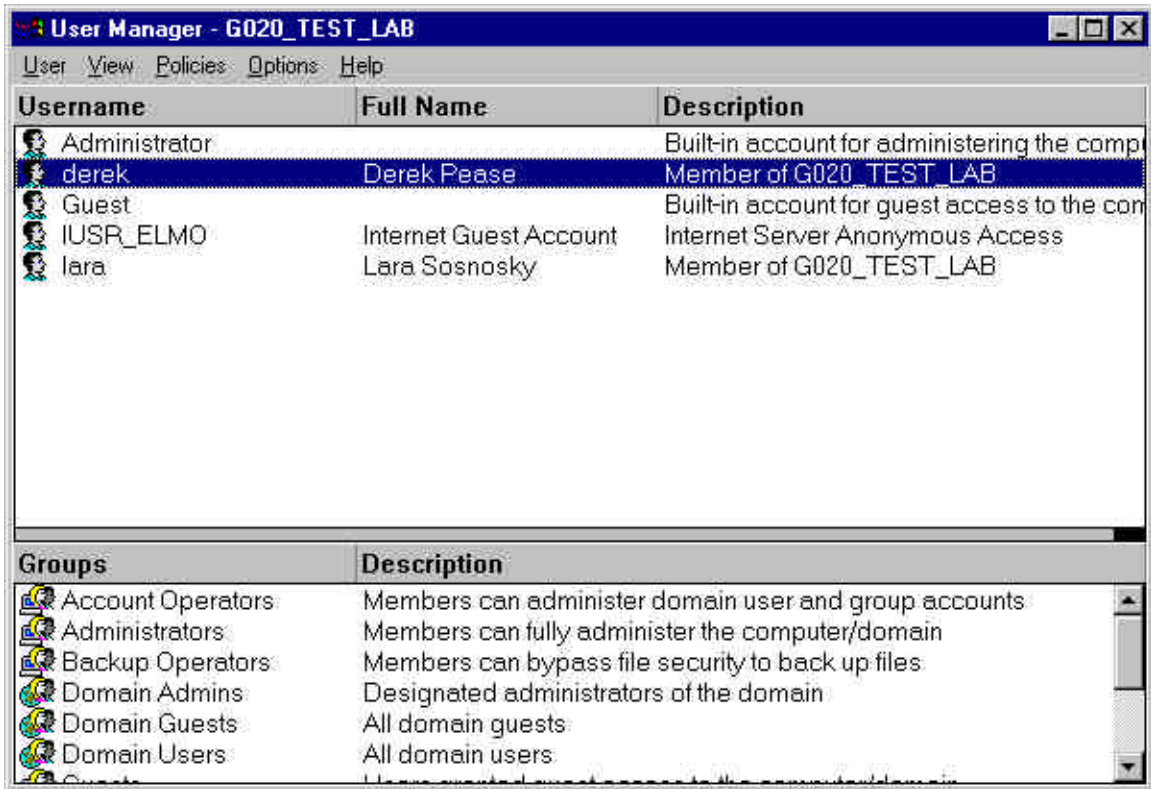
Before creating user accounts, the group or domain for which the account will be a member must already exist. Each group will contain users with similar job roles and privileges.

Table 9-1 lists the steps for using the User Manager for Domains tool to create new groups and user accounts and assign account restrictions. These steps should be performed on the PDC and not on individual workstations. The Navigate column lists the directions to view and open system windows. The Procedure column lists the options for each step of the configuration. The Rationale column explains the reasoning behind each procedure.

**Table 9-1. User Manager for Domains Configuration Procedures**

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
1.	In the Taskbar, click on the Start button, Programs, Administrative Tools, then User Manager for Domains. When the User Manager for	In the New Global Group window (Figure 9-2), type in a unique group name in the Group Name area using the IT-21 standard (e.g., "Privileged Users").	As new users are created (step 2 below), they can be added to this group which gives them more privileges that will be defined in the System Policy section.

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
	Domains window appears (Figure 9-1) select the User menu item, then the New Global Group item.	Skip the Description box. Select users in the right-hand list and click on the Add button to make them group members. Click OK when all users have been added.	
2.	In the User Manager for Domains window, select the User menu item, then the New User item.	When the New User window appears (Figure 9-3), do the following:  In the Username area, give the user a unique username using the IT-21 standard (e.g., "NavyUser").  Skip the Full Name and Description boxes.  In the Password area, enter the default new user password.  Reenter the default new user password in the Confirm Password box.  Check User Must Change Password at Next Logon.  Ensure the other three check boxes (User Cannot Change Password, Password never expires, Account Disabled) are not checked.  Click Add.	Preferably, usernames are between 8 and 20 characters in length.  This password will be replaced when the new user logs on for the first time.



**Figure 9-1. User Manager Window**

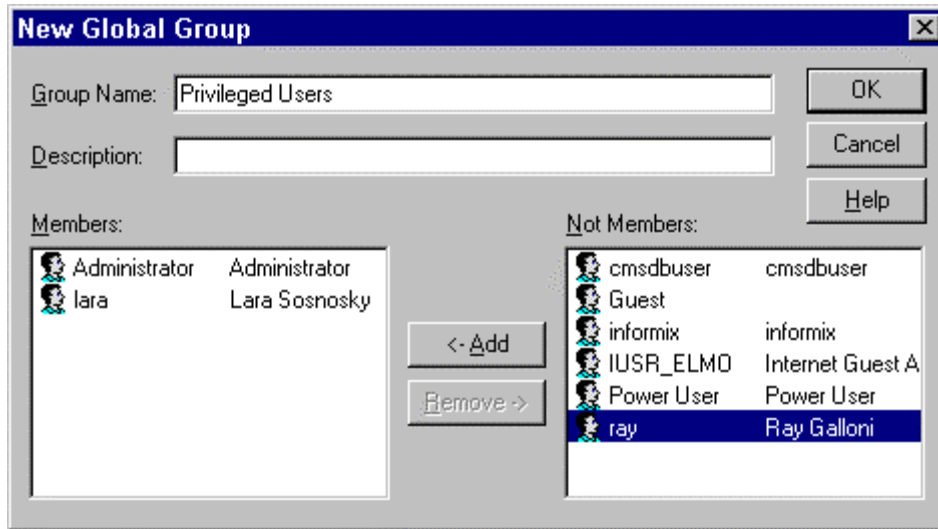


Figure 9-2. New Global Group Window

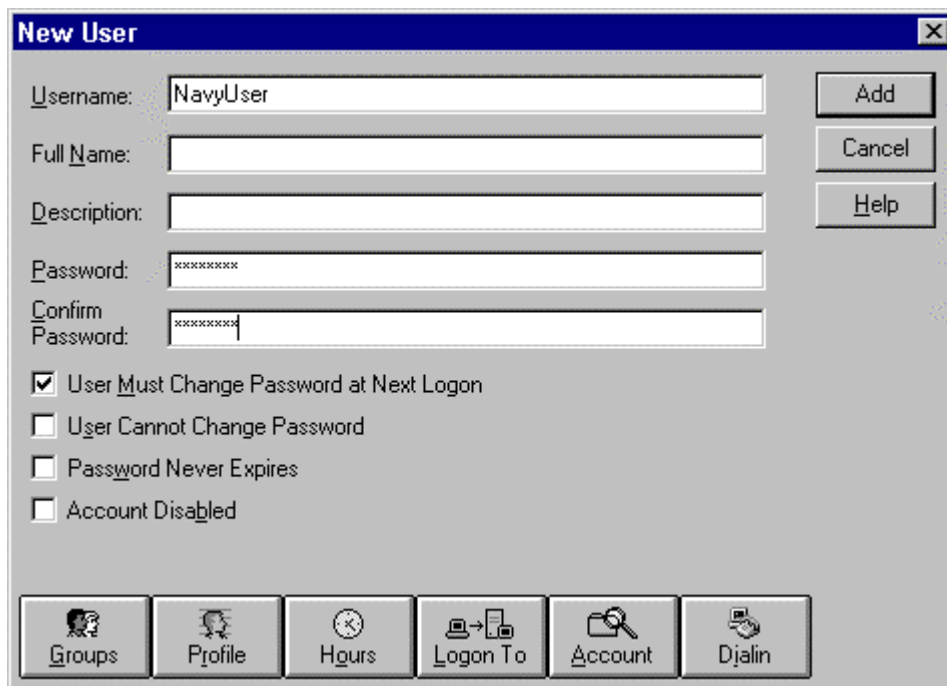


Figure 9-3. New User Window

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
3.	In the User Manager for Domains window, double-click on the username you added in step 1.	<p>In the User Properties window, click on the Group menu item at the bottom of the window. When the Group Memberships window appears, do the following:</p> <p>Assign the new user membership to the appropriate existing group(s) by selecting the group in the list on the right and clicking the Add button.</p> <p>Click OK.</p> <p>Click on the Account menu item. When the Account window appears, do the following:</p> <p>Note the Account Type field with the option of creating either a local account or a global account.</p> <p>Repeat for as many users as required.</p>	<p>The user will be added to the specified group.</p> <p>Users should only be members of groups that are necessary for performing their work.</p> <p>The use of local accounts for users of untrusted domains is discouraged.</p>
4.	Select User and then New User from the User Manager for Domains menu.	Create a user with Domain Administrative privileges (i.e., belongs to the Domain Admins group).	<p>The default Administrator account is not subject to failed logon lockout. This feature, along with its considerable privileges, makes it an attractive target for attacks.</p> <p>The next few steps will address renaming and</p>

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
			<p>removing the privileges of the default Administrator account. Removing the privileges is necessary since certain attack tools (e.g., Red Button) can identify the default Administrator account by its user identifier (UID) even after it has been renamed. The UID of any account does not change after being renamed.</p> <p>Before removing the default Administrator account from the Domain Admins group, another account with Administrative privileges must exist.</p>
5.	<p>In the User Manager for Domains window, click on the Administrator account username.</p> <p>Click on the menu item User, then select Rename.</p>	<p>When the Rename window appears, type “&lt;machine name&gt;_admin” in the Change To: box, then click OK.</p>	<p>Renaming the account protects the system from intruders knowing the Windows NT default Administrator username.</p>
6.	<p>Double-click on the newly renamed Administrator account.</p>	<p>Ensure there is no data in the Full Name field.</p> <p>Select the entire field for Description. Press the backspace key to erase any text in this field.</p> <p>Click OK.</p>	<p>Removing the account description protects the system from intruders recognizing the Windows NT default Administrator account.</p>
7.	<p>Double-click on</p>	<p>In the Local Group</p>	<p>This step adds the</p>

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
	“Administrators” in the Group window.	Properties window, click on the Add button. Highlight the newly renamed default Administrator name in the Names list and click Add. Click OK. The default Administrator account should now be listed as a member of the local Administrators group. Click OK.	renamed default Administrator account to the local Administrators group on the PDC.
8.	Double-click on the renamed default Administrator account. In the User Properties window, click on the Groups button.	Highlight all groups except the local Administrators group and click Remove. Click OK.	This step removes the default Administrator account from the Domain Admins group, so that it is only a member of the local Administrators group on the PDC.
9.	In the User Properties window, click on the Hours button.	Highlight all of the bars for each day of the week and click on the Disallow button. Click OK.	This step prevents the default Administrator account from logging in to the domain.

### **Other User Account Recommendations:**

Ensure users and groups have the least privileges necessary to perform their work duties. Normal users should only have a single, domain-based account. Privileged users should have a non-privileged account in addition to their privileged account.

Individual accountability must be enforced for every person using a Navy system in the form of a user identifier (UID) and password-protected account. No more than one person should have access to any single account.

If Guest accounts are not required on the server or workstation, disable them through the User Manager tool. If Guest accounts are required, at a minimum do the following:

- Choose strong passwords for each Guest account and change them regularly.

- Provide different, non-standard name(s) for this account (including the Guest built-in account).
- Ensure that the Guest accounts have no privileges and a minimum set of rights.
- Prohibit the Guest from becoming a member of Domain Users or any other group.
- Monitor the Guest's intruder detection status.
- NOTE: Several possible Guest accounts could be used on a Windows NT system. IIS creates a Guest account on the server, as does Structured Query Language (SQL) Server, in addition to the built-in Guest accounts created on both server and workstation nodes.

Periodically check the system for user accounts that have been inactive for a long period of time and disable them. Disabling those accounts, but not deleting, will allow them to be more easily reactivated at a later time should it become necessary. If a user account is no longer needed (e.g., user leaves the department, user changes job duties) the account should be deleted in the User Manager for Domains. Deleting an account will permanently erase the SID associated with the UID, and all privileges formally granted to this account can never be restored even if a new account with the same name is created.

## **Section 10**

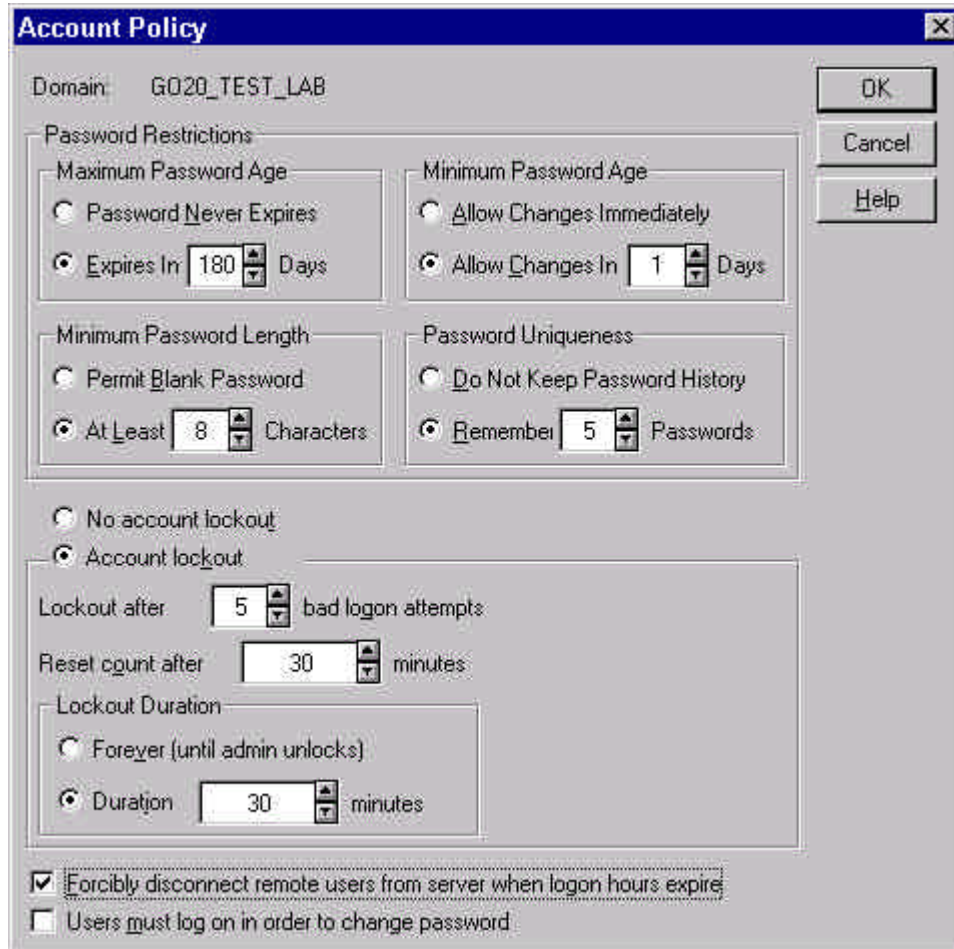
# **User Account Policy Configuration**

Follow the procedures in Table 10-1 to set up account policy procedures. The following steps should be performed on the PDC and not on individual workstations. The Navigate column lists the directions to view and open system windows. The Procedure column lists the options for each step of the configuration. The Rationale column explains the reasoning behind each procedure.

**Table 10-1. Account Policy Configuration Procedures**

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
1.	In the Taskbar, click on the Start button, Programs, Administrative Tools, and then User Manager for Domains. When the User Manager for Domains window appears, select the Policies menu item and then Account.	<p>When the Account Policy window appears (Figure 10-1), do the following:</p> <p>In the Maximum Password Age area, set Expires In 180 Days.</p> <p>In the Minimum Password Age area, set Allow Changes In 1 Days.</p> <p>In the Minimum Password Length area, set At Least 8 Characters.</p> <p>In the Password Uniqueness area, set Remember 5 Passwords.</p> <p>Set Account lockout on; Lockout after 5 bad logon attempts, Reset count after 30 minutes, set Duration 30 minutes.</p>	<p>Passwords must not be allowed to never expire.</p> <p>Password Uniqueness prevents the user from using the same password consecutively.</p> <p>A long password of at least 8 characters puts a restraint on an intruder attempting to crack passwords.</p> <p>Setting logon hours limits out-of-hour use on the system.</p> <p>NOTE: Make sure the Start toolbar is not in the way of the last two boxes (“Forcibly disconnect ...” and “Check Users ...”) found at the bottom of the Account Policy window.</p>

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
		<p>Check Forcibly disconnect remote users from server when logon hours expire. Do NOT check Users must log on in order to change password.</p> <p>Click OK.</p>	<p>Administrators may want to check the “Users must log on in order to change password” option AFTER new users have logged in for the first time and changed their password. This option must not be checked while the “User must change password at next logon” option is enabled (Table 9-1, step 2) until the new user has performed an initial logon.</p>



**Figure 10-1. Account Policy Window**

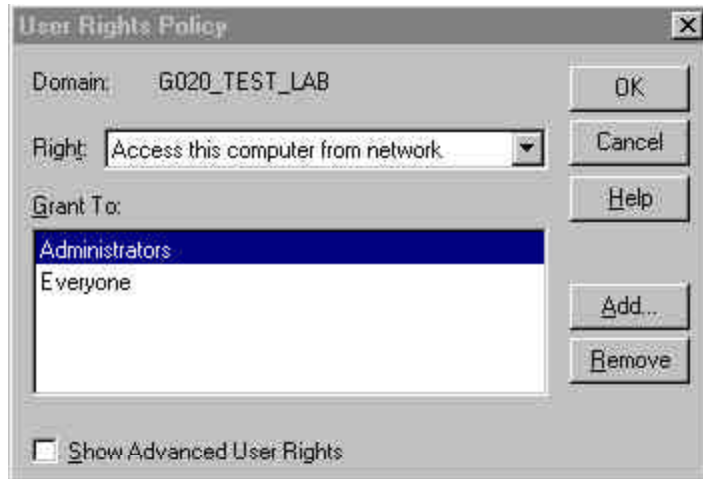
## Section 11

# User Rights Policy Configuration

Follow the procedures in Table 11-1 to set up the user rights policy. The following steps should be performed on the PDC and all individual workstations. The Navigate column lists the directions to view and open system windows. The Procedure column lists the options for each step of the configuration. The Rationale column explains the reasoning behind each procedure.

**Table 11-1. User Rights Policy Configuration Procedures**

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
1.	<p>In the Taskbar, click on the Start button, Administrative Tools, and then User Manager for Domains (on servers) or User Manager (on workstations).</p> <p>When the User Manager window appears, select the Policies menu item and then User Rights.</p> <p>When the User Rights Policy window appears (Figure 11-1), check Show Advanced User Rights.</p>	<p>Select each right one at a time from the “Right” drop-down list.</p> <p>Ensure that only the user rights listed in Table 11-2 and Table 11-3 are assigned to the appropriate users.</p>	<p>Providing only the rights necessary for groups and individual users to perform their work duties will help ensure a high level of security.</p>



**Figure 11-1. User Rights Policy Window**

The user rights policy for Navy Windows NT servers is defined in Table 11-2. The user rights policy for Navy Windows NT workstations is defined in Table 11-3. The User Rights Policy column lists each right that can be assigned to a user. The Policy column lists each right that can be assigned to a user. The “R” or “A” in this column symbolizes whether the user right is regular or advanced. The Windows NT Server (NTS) Default column lists the users who are assigned the right in the User Rights Policy column by default. The Navy Configuration column lists the users that should be assigned the right listed in the Policy column. Blank columns indicate no users are specified by default.

Service Pack 3 introduces a new BUILTIN group called Authenticated Users. The Authenticated Users group is similar to the Everyone group, except for one important difference: anonymous logon users (or NULL session connections) are never members of the Authenticated Users group. Using this group in place of the Everyone group improves the overall security of the domain.

**Table 11-2. User Rights Policy for NT Servers**

	<b>Policy [Regular (R), Advanced (A)]</b>	<b>NTS Default</b>	<b>Navy Configuration</b>
1.	Access this computer from the network (R)	Administrators Everyone	Administrators Everyone

	<b>Policy [Regular (R), Advanced (A)]</b>	<b>NTS Default</b>	<b>Navy Configuration</b>
2.	Act as part of the operating system (A)		
3.	Add workstations to domain (R)		
4.	Back up files and directories (R)	Administrators Backup Operators Server Operators	Administrators Backup Operators Server Operators
5.	Bypass traverse checking (A)	Everyone	Everyone
6.	Change the system time (R)	Administrators Server Operators	Administrators Server Operators
7.	Create a pagefile (A)	Administrators	Administrators
8.	Create a token object (A)		
9.	Create permanent shared objects (A)		
10.	Debug programs (A)	Administrators	Administrators
11.	Force shut down from a remote system (R)	Administrators Server Operators	Administrators Server Operators
12.	Generate security audits (A)		
13.	Increase quotas (A)	Administrators	Administrators
14.	Increase scheduling priority (A)	Administrators	Administrators
15.	Load and unload device drivers (R)	Administrators	Administrators
16.	Lock pages in memory (A)		

	<b>Policy [Regular (R), Advanced (A)]</b>	<b>NTS Default</b>	<b>Navy Configuration</b>
17.	Log on as a batch job (A)		
18.	Log on as a service (A)		
19.	Log on locally (R)	Account Operators Administrators Backup Operators Print Operators Server Operators	Account Operators Administrators Backup Operators Print Operators Server Operators
20.	Manage auditing and security log (R)	Administrators	Administrators
21.	Modify firmware environment values (A)	Administrators	Administrators
22.	Profile single process (A)	Administrators	Administrators
23.	Profile system performance (A)	Administrators	Administrators
24.	Replace a process level token (A)		
25.	Restore files and directories (R)	Administrators Backup Operators Server Operators	Administrators Backup Operators Server Operators
26.	Shut down the system (R)	Account Operators Administrators Backup Operators Print Operators Server Operators	Account Operators Administrators Backup Operators Print Operators Server Operators
27.	Take ownership of files or other objects (R)	Administrators	Administrators

The user rights policy for Navy Windows NT workstations is defined in Table 11-3. The User Rights Policy column lists each right that can be assigned to a user. The Policy column lists each right that can be assigned to a user. The “R” or “A” in this column symbolizes

whether the user right is regular or advanced. The Windows NT Workstation (NTW) Default column lists the users who are assigned the right in the User Rights Policy column by default. The Navy Configuration column lists the users that should be assigned the right listed in the Policy column. Blank columns indicate no users are specified by default.

**Table 11-3. User Rights Policy for NT Workstations**

	<b>Policy [Regular (R), Advanced (A)]</b>	<b>NTW Default</b>	<b>Navy Configuration</b>
1.	Access this computer from the network (R)	Administrators Everyone Power Users	Administrators Everyone
2.	Act as part of the operating system (A)		
3.	Add workstations to domain (R)		
4.	Back up files and directories (R)	Administrators Backup Operators	Administrators Backup Operators
5.	Bypass traverse checking (A)	Everyone	Everyone
6.	Change the system time (R)	Administrators Power Users	Administrators
7.	Create a pagefile (A)	Administrators	Administrators
8.	Create a token object (A)		
9.	Create permanent shared objects (A)		
10.	Debug programs (A)	Administrators	Administrators
11.	Force shut down from a remote system (R)	Administrators Power Users	Administrators
12.	Generate security audits (A)		

	<b>Policy [Regular (R), Advanced (A)]</b>	<b>NTW Default</b>	<b>Navy Configuration</b>
13.	Increase quotas (A)	Administrators	Administrators
14.	Increase scheduling priority (A)	Administrators Power Users	Administrators
15.	Load and unload device drivers (R)	Administrators	Administrators
16.	Lock pages in memory (A)		
17.	Log on as a batch job (A)		
18.	Log on as a service (A)		
19.	Log on locally (R)	Administrators Backup Operators Everyone Guests Power Users Users	Administrators Backup Operators Authenticated Users
20.	Manage auditing and security log (R)	Administrators	Administrators
21.	Modify firmware environment values (A)	Administrators	Administrators
22.	Profile single process (A)	Administrators Power Users	Administrators
23.	Profile system performance (A)	Administrators	Administrators
24.	Replace a process level token (A)		
25.	Restore files and directories (R)	Administrators Backup Operators	Administrators Backup Operators

	<b>Policy [Regular (R), Advanced (A)]</b>	<b>NTW Default</b>	<b>Navy Configuration</b>
26.	Shut down the system (R)	Administrators Backup Operators Everyone Power Users Users	Administrators Backup Operators Users
27.	Take ownership of files or other objects (R)	Administrators	Administrators

## Section 12

# Domain Model Configuration (Trust Relationships)

Consult with your System Administrator to choose the proper domain model for your site. See the *Microsoft Windows NT Server Version 4.0 Concepts and Planning* manual for details.

The user accounts, profiles, logon scripts, and home directories should be placed at the domain controller level so user environments can be centrally managed.

Several users can be added to a group in which their configurations and restrictions can be centrally controlled. Windows NT recognizes two types of groups: local and global. Pay particular attention to local groups that contain users from untrusted domains.

Allow only domain user accounts on the network. A node should not contain any local user accounts, other than the two built-in local accounts (the Administrator and disabled Guest accounts). Domain user accounts can be controlled by placing appropriate files in the Netlogon directory of the domain controllers, such as the default user profile or system policy.

Roaming profiles allow users to log onto other workstations within their domains. These profiles are allowed, but cached data from a roaming profile must be deleted from the workstation or server once the user has logged out of the server.

The number of workstations that can be accessed by a user should be limited. Preferably, each user should only log onto his or her desktop machine to prevent users from unnecessary roaming.

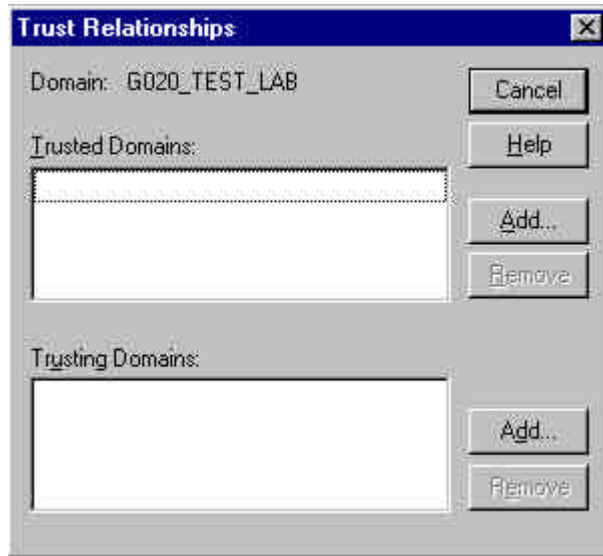
Domains should be used to separate Internet and Intranet networks. Never place Internet resources in a domain that contains Intranet resources and vice versa. The Intranets should also be protected from Internets via hardware, such as a router, firewall, and/or proxy server.

Trust relationships can be created to allow access to resources in other domains. Two types of trust relationships can be set up between any two domains: one-way trust and two-way trust. Using this trust model, up to six trust relationships can exist among three domains, twelve among four domains, and so forth. To prevent a complicated trust policy and make the trust relationships more manageable, their number should be kept to a minimum. Also, if possible, use only one-way trust relationships when that model can meet requirements. Minimize the use of two-way trust relationships to those instances in which it is required.

Table 12-1 lists the steps taken to set up and remove trust relationships in your domain. The following steps should be performed on the PDC. The Navigate column lists the directions to view and open system windows. The Procedure column lists the options for each step of the configuration. The Rationale column explains the reasoning behind each procedure.

**Table 12-1. Domain Model Configuration Procedures**

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
1.	<p>In the Taskbar, click on the Start button, Programs, Administrative Tools, and then User Manager for Domains.</p> <p>When the User Manager window appears, select the Policies menu item, and then select the Trust Relationships menu item.</p>	<p>When the Trust Relationships window appears (Figure 12-1), do the following:</p> <p>To add a trusting domain, select the Add option by the trusting domain window. When the Add Trusting Domain window appears, enter the name of the trusting domain in the Domain field. Enter and confirm the password for use by the other domain's Administrator. Click OK.</p> <p>To add a trusted domain, select the Add option in the trusted domain window. When the Add Trusted Domain window appears, enter the name of the domain to be trusted in the Domain field. Enter the password obtained from the Administrator of the trusted domain. Click OK.</p>	<p>Establishing a trust relationship requires two steps performed in two distinct domains.</p> <p>The domain that will be the trusted domain must first add a domain to its list of trusting domains. Next, the trusting domain must add the first domain to its list of trusted domains.</p> <p>Establishing a two-way trust relationship (in which each domain trusts the other) requires this procedure to be performed twice, once in each domain.</p> <p>Trust relationships should be avoided unless absolutely necessary.</p>



**Figure 12-1. Trust Relationships Window**

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
2.	To remove trust relationships, follow the instructions in the Navigation column of step 1 above to invoke the Trust Relationships window.	<p>To remove a trusting domain, select the domain in the Trusting Domains box and click on the Remove button. Click Yes.</p> <p>To remove a trusted domain, select the domain in the Trusted Domains box and click on the Remove button. Click Yes.</p>	Removing a two-way trust relationship requires these steps to be performed on the domain controllers in their separate domains.

## Section 13

# User Environment Profile Configuration

System policies and user profiles have a substantial impact on the security of the system. They form a hierarchical structure of controls for the work environment and desktop settings for users. The hierarchy ranges from the user profile controlled by the individual user on the low security end to the system policy in which the work environment for all users can be controlled by the System Administrator.

This section describes how to define user profiles for critical global user groups and assign a profile to each user. This approach was selected to avoid the labor-intensive prospect of managing individual user profiles. The key global groups defined in this section are Domain Users, Privileged Users, and Domain Admins. These groups were selected to take advantage of default groups created when Windows NT is installed and for which file permissions have already been set.

A shared UID will allow numerous users to utilize the same account and password. Each user who has access to this shared UID will also share the UID's profile. Consequently, all users accessing the domain through this shared UID will share operating environments, Web browser bookmarks, and even digital authentication certificates. Hence, the use of shared UIDs is strongly discouraged.

Table 13-1 lists the steps for adding a Privileged Users group and configuring a user's profile for each new account created. The Navigate column lists the directions to view and open system windows. The Procedure column lists the options for each step of the configuration. The Rationale column explains the reasoning behind each procedure.

**Table 13-1. User Profile Configuration Procedures**

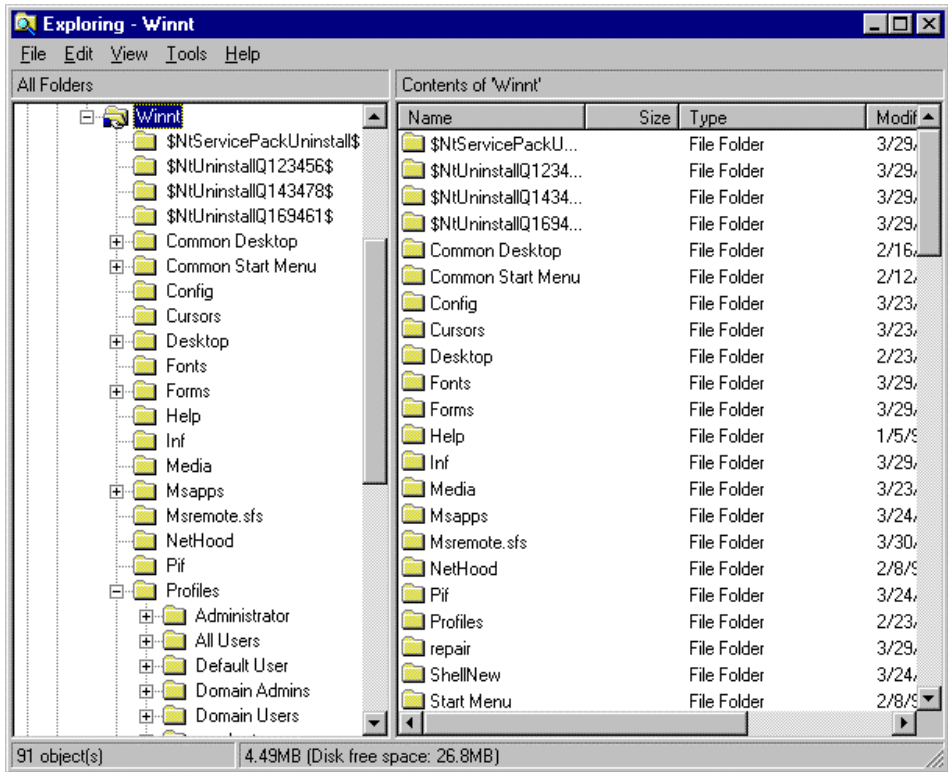
	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
1.	Refer to step 1 in Section 9 for creating a new global group.	Create a global group called "Privileged Users." Add the appropriate users to this group.	Windows NT servers do not contain the Power Users group that NT workstations have by default. The Privileged Users group will contain more privileges than Domains Users but less than Domain

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
			Administrators.
2.	<p>On the fileserver selected to host user home directories, click on the Start button, Programs, then Windows NT Explorer.</p> <p>Choose a drive letter to create the users' home directories. Name this folder "Users". Right click on this folder, select Properties, and then select the Sharing tab.</p>	<p>Select "Shared As" and click on the New Share button. Type "USERS\$" in the Share Name field. Click OK.</p> <p>Click on Permissions.</p> <p>Click Add in the "Access Through Share Permissions" window.</p> <p>Select the three groups (Domain Admins, Domain Users, and Privileged Users) and click Add after each one is highlighted.</p> <p>Change the "Type of Access" from "Read" to "Change."</p> <p>Click OK.</p> <p>Highlight the group "Everyone" and select "Remove."</p> <p>Highlight the group "Domain Admins" and change the "Type of Access" from "Change" to "Full Control."</p> <p>Click OK in the "Access Through Share Permissions" window.</p> <p>Click Apply and then OK.</p>	<p>Creates the location for user home directories for your domain and creates a hidden share for this directory so it can be mapped over the network.</p> <p>The share is configured to restrict access to only the three primary user groups.</p>
3.	<p>On the PDC, click on the Start button,</p>	<p>When the Profiles window appears, do the</p>	<p>Every user must have a profile on the PDC.</p>

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
	<p>Programs, Administrative Tools, and then User Manager for Domains.</p> <p>When the User Manager window appears, double-click on a user listed. When the User Properties window appears, click on the Profiles icon at the bottom of the window.</p> <p>Repeat for all new users.</p>	<p>following:</p> <p>In the User Profiles area, type in the following path name: “\\&lt;PDC_NAME&gt;\Profile\$\%username%.”</p> <p>In the Home Directory area select “Connect” and choose a drive letter from the drop-down list. In the “To” box, type in the following path name: “\\&lt;fileserver&gt;\users\$\%username%.”</p> <p>Click OK.</p>	<p>The home directory of every user should reside on a domain fileserver and not on a domain controller (PDC or BDC).</p>
4.	<p>This step should be performed on the PDC. In the Taskbar, click on the Start button, Programs, then Windows NT Explorer. When the Exploring window appears, click on the plus box next to the &lt;%systemroot%&gt; folder. Continue to traverse the directory structure by clicking on the plus box next to the Profiles folder (see Figure 13-1).</p>	<p>Single-click on the Profiles folder. Select File, New, then Folder from the menu bar. Create three new folders and name them Domain Users, Privileged Users, and Domain Admins.</p> <p>Double-click on the Default User folder and then in the right window, highlight only the folders by holding down the Control key and clicking on each folder. Right-click on the highlighted folders and select “Copy.” Right-click on each of the newly created group folders and select “Paste.”</p>	<p>Creates three new profile folders for each group. The profile configuration for the Default User is used as the baseline to modify the profiles for the user groups.</p>
5.	<p>In the left pane of the</p>	<p>Highlight the</p>	<p>Prepare to move these</p>

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
	Exploring window, click the plus box next to the “All Users” folder, and then click the plus box next to the “Start Menu” folder. Click on the “Programs” folder.	“Administrative Tools (Common)” and “Microsoft Internet Server (Common)” (if installed) and choose Copy from the Edit menu.	two folders to the Domain Admins profile folder. These tools are not needed by Domain Users or Privileged Users.
6.	Double-click on the new “Domain Admins” folder. Click on the plus box next to the “Start Menu” folder. Click on the “Programs” folder.	Select Paste from the Edit menu.	Gives the Domain Admins group the necessary administrative tools.
7.	Click on the “Programs” folder in the “All Users” profile folder.	Highlight the “Administrative Tools (Common)” and “Microsoft Internet Server (Common)”. Delete both of these folders.	Removes these tools from the desktop for both the Domain Users and Privileged Users groups.
8.	In the Exploring window, right-click on the “Profiles” folder, select Properties, and then select the Sharing tab.	Select “Shared As” and type “Profile\$” for the Share name. Click on “Permissions.” In the “Access Through Share Permissions” window, click Add.  Select the three groups (Domain Admins, Domain Users, and Privileged Users) and click Add after each one is highlighted. Click OK.  Highlight the group “Everyone” and select “Remove.” Highlight the	Creates a hidden share for this directory so it can be accessed over the network. The share is configured to restrict access to only the three primary user groups.  The share name must be 8 characters or less (including the “\$”) so that the share can be read by other non-Windows NT machines.

	Navigate	Procedure	Rationale
		<p>group “Domain Admins” and change the “Type of Access” from “Change” to “Full Control.”</p> <p>Click OK in the “Access Through Share Permissions” window.</p> <p>Click Apply and then OK in the “Profiles Share Window.”</p>	



**Figure 13-1. Windows NT Explorer - “%systemroot%\Profiles” Folder**

The final step in this section is to update the file and directory permissions for the Profiles folder. Generally, first assign the lowest level of permissions and propagate that throughout the entire folder. Next, assign specific permissions to specific subfolders. Finally, revise the permissions for the parent folder (Profiles) without propagating the changes to the subfolders. Table 13-2 describes the steps to update the file and directory permissions for the Profiles folder. The Navigate column lists the directions to view and open system windows. The Procedure column lists the options for each step of the configuration. The Rationale column explains the reasoning behind each procedure.

**Table 13-2. File and Directory Permissions for the Profiles Folder**

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
1.	Right-click on the “Profiles” folder and select Properties. Click on the Security tab and then click Permissions.	<p>Check the “Replace Permissions on Subdirectories” and “Replace Permissions on Existing Files” blocks. Click Add. Ensure that the proper domain name is shown in the “List Names From:” drop-down list. Select the following groups to add:</p> <p>CREATOR OWNER            Domain Admins            Domain Users            Privileged Users            SYSTEM</p> <p>Select “Read” as the “Type of Access” (see Figure 13-2). Click OK.</p> <p>Highlight the following groups in succession and change the “Type of Access” to “Full Control”:</p> <p>CREATOR OWNER            Domain Admins</p>	Establishes the basic level of permissions for the Profiles folder and propagates these permissions to all subfolders and files.

	Navigate	Procedure	Rationale
		<p>SYSTEM</p> <p>Highlight the Everyone group and click Remove. Verify that your settings are correct and click OK. Click Yes in the subsequent warning dialog box. Click OK.</p>	

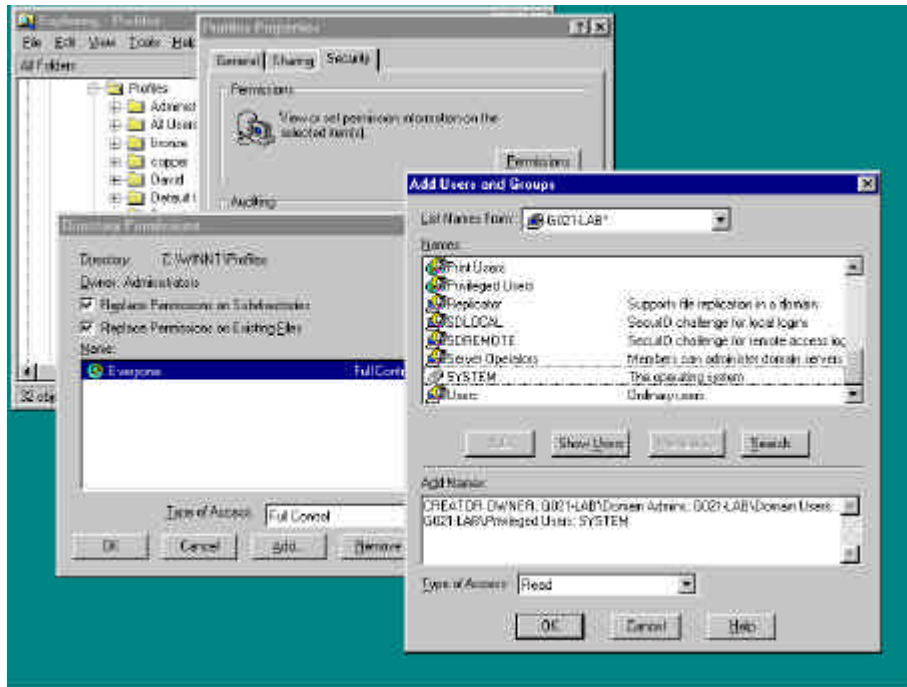
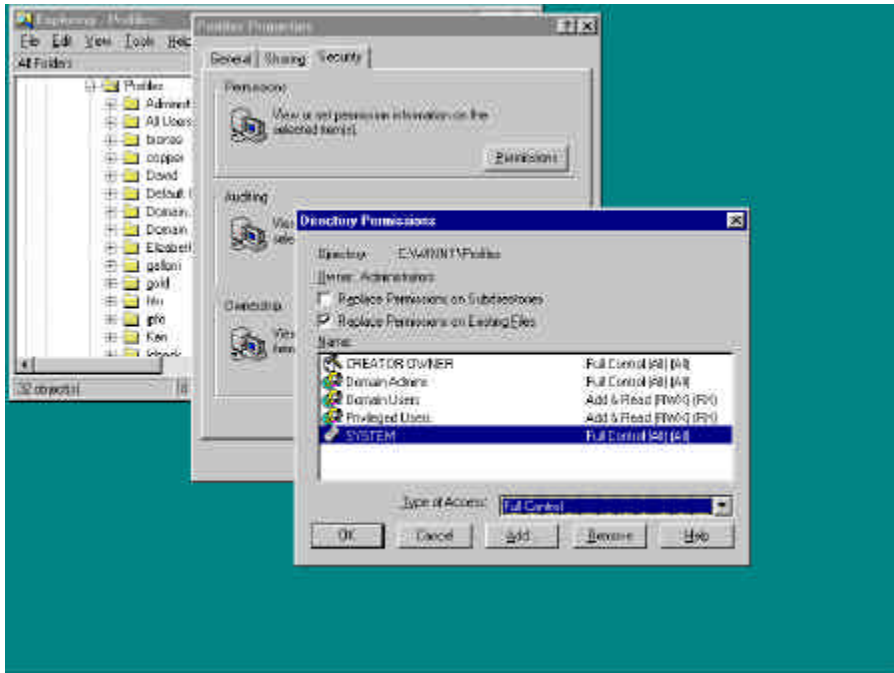


Figure 13-2. Window NT Explorer - Initial Permissions on Profiles Folder

	Navigate	Procedure	Rationale
2.	<p>Right-click on the “Domain Admins” folder and select Properties. Click on the Security tab</p>	<p>Check the “Replace Permissions on Subdirectories” and “Replace Permissions on</p>	<p>Protects the Domain Admins profile by removing all access to this folder from lower</p>

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
	and then click Permissions.	Existing Files” blocks. Remove the Domain Users and Privileged Users groups from the list of groups with directory permissions. Verify that your settings are correct and click OK. Click Yes in the subsequent warning dialog box. Click OK.	authority groups.
3.	Right-click on the “Privileged Users” folder and select Properties. Click on the Security tab and then click Permissions.	Check the “Replace Permissions on Subdirectories” and “Replace Permissions on Existing Files” blocks. Remove the Domain Users group from the list of groups with directory permissions. Verify that your settings are correct and click OK. Click Yes in the subsequent warning dialog box. Click OK.	Protects the Privileged Users profile by removing all access to this folder from lower authority groups.
4.	Right-click on the “Profiles” folder and select Properties. Click on the Security tab and then click Permissions.	<b>DO NOT PROPAGATE THESE CHANGES TO SUBDIRECTORIES.</b> Ensure that “Replace Permissions on Subdirectories” is NOT checked and “Replace Permissions on Existing Files” IS checked. Highlight the following	Grants the permission necessary for individual user profiles to be created when new users logon for the first time.

	Navigate	Procedure	Rationale
		<p>groups in succession and change the “Type of Access” to “Add &amp; Read”:</p> <p>Domain Users Privileged Users</p> <p>Verify that your settings are correct (see Figure 13-3). Click OK.</p>	



**Figure 13-3. Windows NT Explorer - Final Permissions on Profiles Folder**

## Section 14

# System Policy Configuration

This section describes how to secure the system policy for the entire domain. As described in Table 14-6 later in this section, changes outlined in this section should be made on each controller of a domain. The system policy should be edited on the PDC. No system policies should be placed on any local workstations or standalone servers.

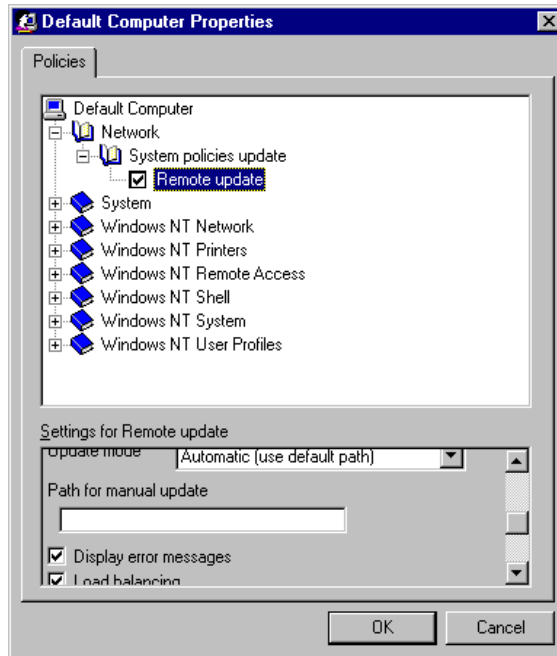
Throughout this section, reference is made to the three possible settings for system policy items. These settings are characterized by grayed-out blocks, solid white blocks, or checked blocks, and can be changed by clicking on each policy block. The solid white block and checked block indicate that Windows NT will write a value in the Registry of the local host. A checked block is an affirmative response to the statement and a solid white block is a negative response to the statement. Conversely, the grayed-out block indicates that Windows NT will not write a value to the Registry, but will instead accept the existing value.

This convention can cause unpredictable results depending on the sequence users log onto the local host. Specifically, if a certain policy setting for the Domain Admins group is left grayed-out and that same setting is checked for the Domain Users group, a Domain Admin who logs in after a Domain User may inherit a restricted policy. For instance, if the Domain Users group was specifically denied a permission (e.g., access to Registry editing tools), the member of the Domain Admins group will also be denied that permission if they log in after a Domain User. This pattern of behavior results because the machine was not rebooted in the interval between their use (i.e., the local Registry was left intact) and the system policy for the Domain Admins group defined that the value of the setting be accepted.

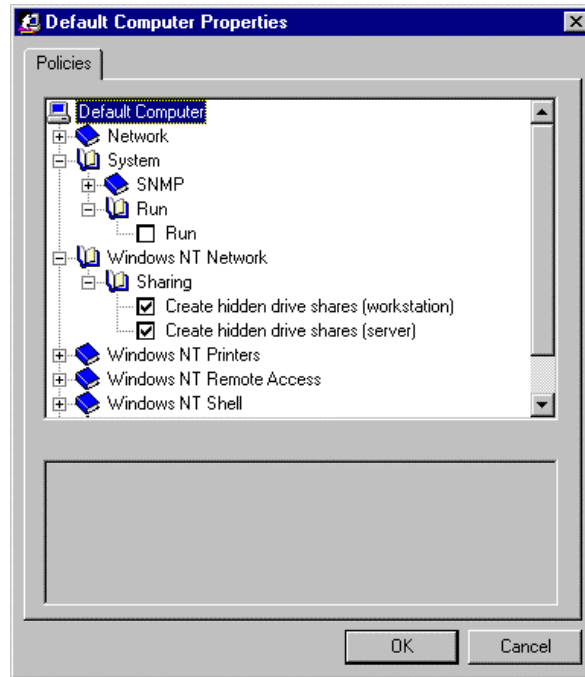
Table 14-1 lists the steps to configure computer properties for user profiles, Windows NT shells, and the Windows NT operating system. This process should be completed in one sitting. Do not save a partially completed configuration, log out, and then log in and continue. Failure to complete these steps at one time may result in a half-implemented policy and may produce undesirable effects. The Navigate column lists the directions to view and open system windows. The Procedure column lists the options for each step of the configuration. The Rationale column explains the reasoning behind each procedure.

**Table 14-1. Default Computer Procedures**

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
1.	<p>On the PDC, click on the Start button and then Run. In the Run window, type in "C:\winnt\poledit.exe" and click OK to start the System Policy Editor.</p> <p>When the System Policy Editor window appears, select the File menu, then New Policy.</p> <p>Double-click on the Default Computer icon.</p> <p>When the Default Computer Properties window appears, click the plus box in front of the Network item, then click the plus box in front of the System policies update item (see Figure 14-1).</p>	<p>Check the "Remote update" item. In the lower dialog box, select "Automatic (use default path)" from the drop-down list as the Update mode. Check the "Display error messages" and "Load balancing" boxes.</p>	<p>Causes Windows NT machines to download the system policy from a domain controller.</p> <p>NOTE: The Administrative Tools will temporarily be unavailable (through the Programs folder) while the system policy is being configured.</p>
2.	<p>Click the plus box in front of the System box, then click the plus box in front of the Run box (see Figure 14-2).</p>	<p>Click the shaded block twice to obtain a solid white block.</p>	<p>This will not run any programs during the system boot process.</p>
3.	<p>Click the plus box in front of Windows NT Network, then click the plus box in front of Sharing (see Figure 14-2).</p>	<p>Replace the shaded blocks with checked blocks on both items.</p>	<p>This will cause the system to create the hidden administrative shares during the system boot process.</p>



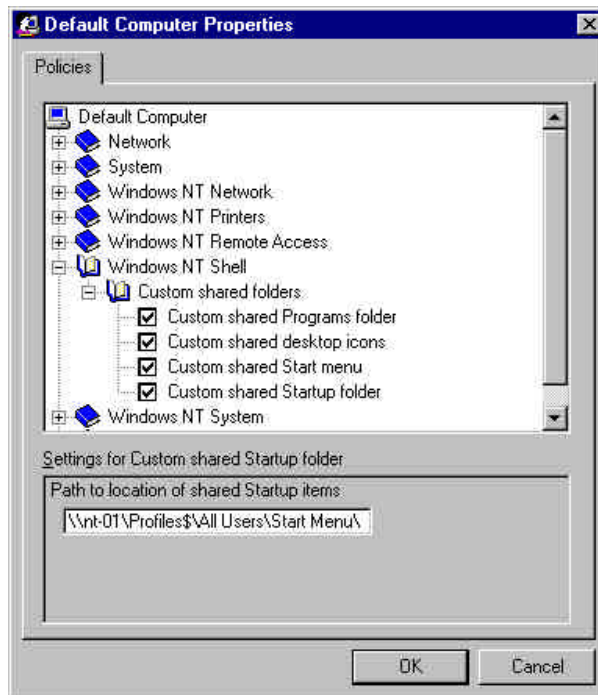
**Figure 14-1. Default Computer Properties - Network**



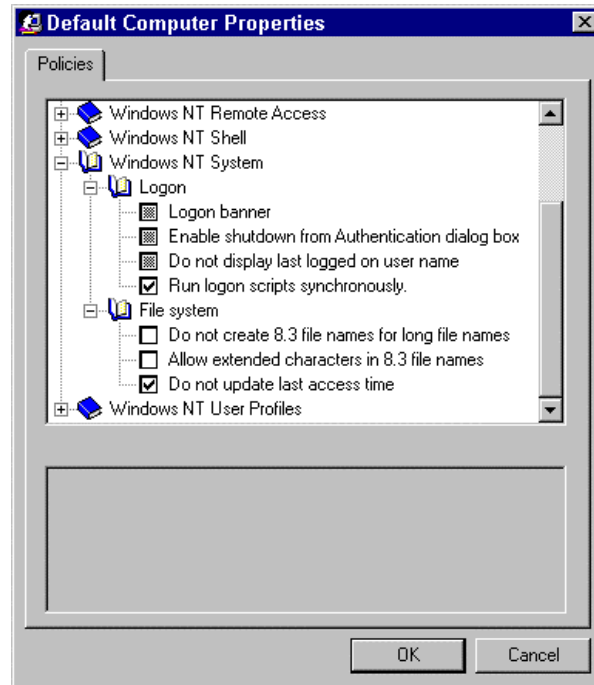
**Figure 14-2. Default Computer System and Windows NT Networking Properties**

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
4.	Click the plus box in front of the Windows NT Shell item, then click the plus box in front of the Custom shared folders item (see Figure 14-3).	<p>Check “Custom shared Programs folder” and enter the following path in the lower dialog box: “\\&lt;PDC NAME&gt;\Profile\$\All Users\Start Menu\Programs.”</p> <p>Check “Custom shared desktop icons” and enter the following path in the lower dialog box: “\\&lt;PDC NAME&gt;\Profile\$\All Users\Desktop.”</p> <p>Check “Custom shared Start menu” and enter the following path in the lower dialog box: “\\&lt;PDC NAME&gt;\Profile\$\All Users\Start Menu\Programs\Startup.”</p> <p>Check “Custom shared Startup folder” and enter the following path in the lower dialog box: “\\&lt;PDC NAME&gt;\Profile\$\All Users\Start Menu.”</p>	Assigns all Domain Users the same Start menu and desktop environment. This allows ease of maintenance for the Administrator. Programs and/or applications can be granted or revoked from Domain Users by editing one user profile.
5.	Click the plus box in front of the Windows NT System item, then click the plus box in front of the Logon item (see Figure 14-4).	Check “Run logon scripts synchronously.”	Performs logon scripts before continuing on with the logon process.

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
6.	Click the plus box in front of the Windows NT System item, then click the plus box in front of the File System item (see Figure 14-4).	<p>Replace the shaded block with a solid white block on the “Do not create 8.3 file names for long file names” and “Allow extended characters in 8.3 file names.”</p> <p>Check “Do not update last access time.”</p>	<p>As an additional security measure, if a penetration is suspected, consider replacing the checked block for the “Do not update last access time” with a solid white block. This will allow the Administrator to determine when each file was last accessed, including when a file was last read. When enacted, system performance is degraded.</p>

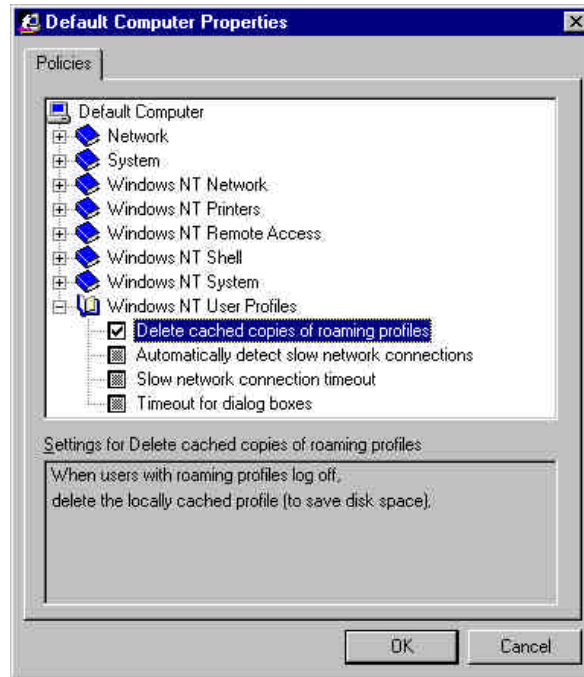


**Figure 14-3. Default Computer Properties - Windows NT Shell**



**Figure 14-4. Default Computer Properties - Windows NT System**

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
7.	Click the plus box in front of the Windows NT User Profiles item (see Figure 14-5).	Check “Delete cached copies of roaming profiles.” Click OK.	Prevents the use of the previous user’s profile.

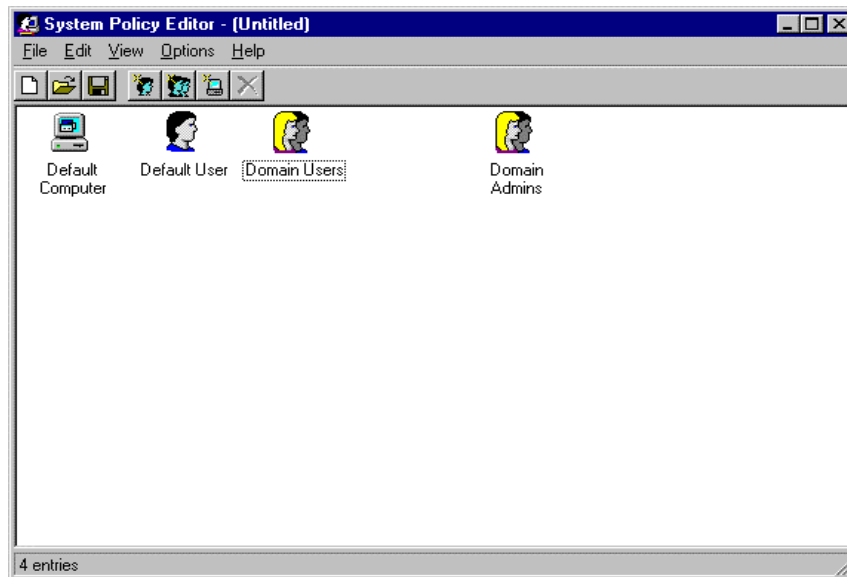


**Figure 14-5. Default Computer Properties - Windows NT User Profiles**

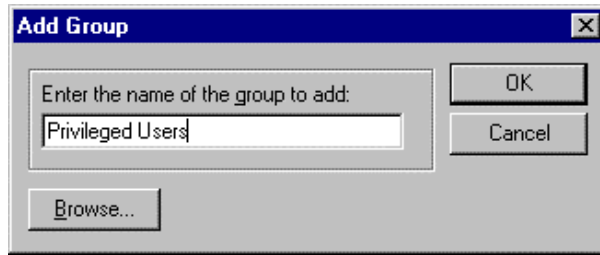
Table 14-2 lists the steps for creating system policies for user groups. The Navigate column lists the directions to view and open system windows. The Procedure column lists the options for each step of the configuration. The Rationale column explains the reasoning behind each procedure.

**Table 14-2. System Policy Editor - User Groups**

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
1.	<p>In the System Policy Editor window, add a system policy icon for the following three groups:</p> <p>Domain Users Privileged Users Domain Admins</p>	<p>Click on the Edit menu and select Add Group. Type in the name of each group and click OK (see Figures 14-6 and 14-7). It is not necessary to create a group icon in the System Policy Editor for every group found in User Manager for Domains.</p>	<p>Control of user access is better administered by using groups versus individual users.</p> <p>Based on the specific environment, additional groups can be defined. The use of three groups provides some granularity of control.</p>



**Figure 14-6. System Policy Editor**



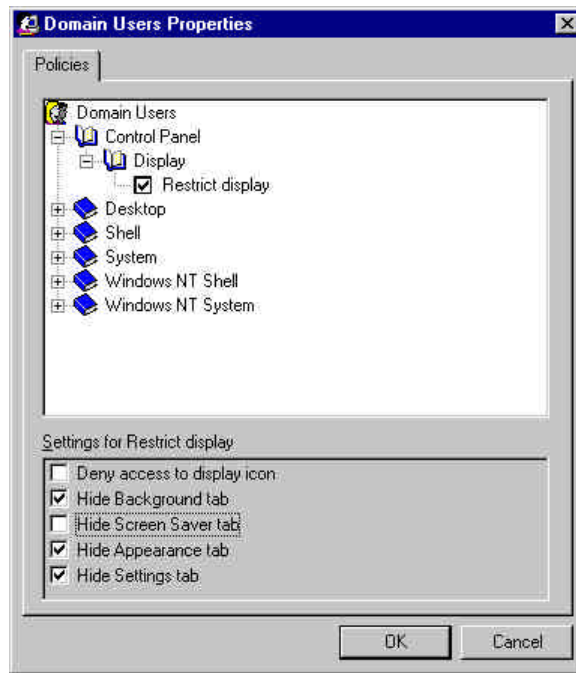
**Figure 14-7. System Policy Editor - Add Group Dialog Box**

Table 14-3 lists the steps for defining the system policy for Domain Users. The Navigate column lists the directions to view and open system windows. The Procedure column lists the options for each step of the configuration. The Rationale column explains the reasoning behind each procedure.

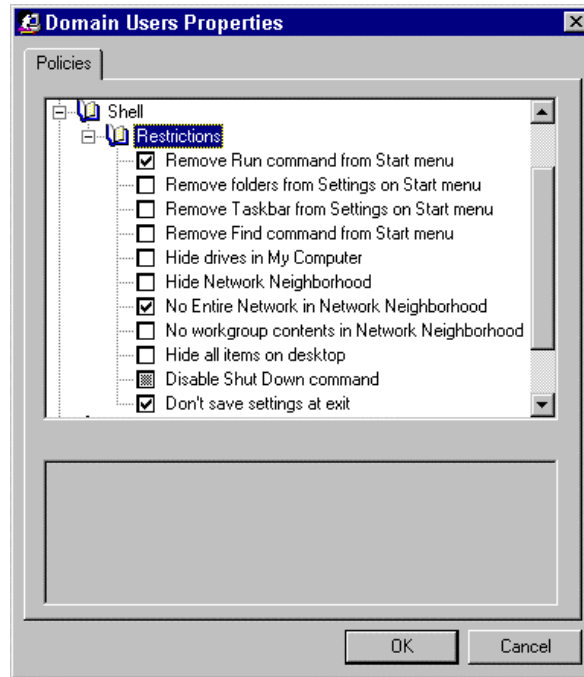
**Table 14-3. Domain Users Properties**

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
1.	Double-click on the Domain Users icon. When the Domain Users Properties window appears, click the plus box in front of the Control Panel item and click the plus box in front of the Display item (see Figure 14-8).	Check “Restrict Display”, which will make the lower dialog box active.  Check “Hide Background tab”, “Hide Appearance tab”, and “Hide Settings tab.”  Keep “Deny access to display icon” and “Hide Screen Saver tab” unchecked.	Each user must configure a password-protected screen saver. Table 15-1 will describe the steps to configure a screen saver through the Control Panel.

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
2.	Click the plus box in front of the Shell item, then click the plus box in front of the Restrictions item (see Figure 14-9).	<p>Replace the shaded blocks with solid white blocks on all selections except:</p> <p>Check “Remove Run Command from Start menu”, “No Entire Network in Network Neighborhood”, and “Don’t save settings at exit.”</p> <p>Keep “Disable Shutdown command” grayed-out.</p>	Prevents Domain Users from running executable commands from the Start menu, browsing the network outside the domain, and making changes that will impact other users.



**Figure 14-8. Domain Users Properties - Control Panel**

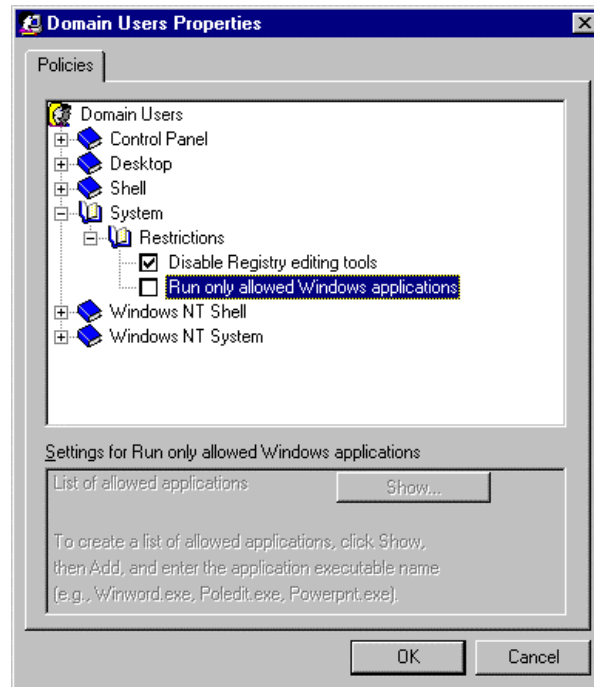


**Figure 14-9. Domain Users Properties - Shell**

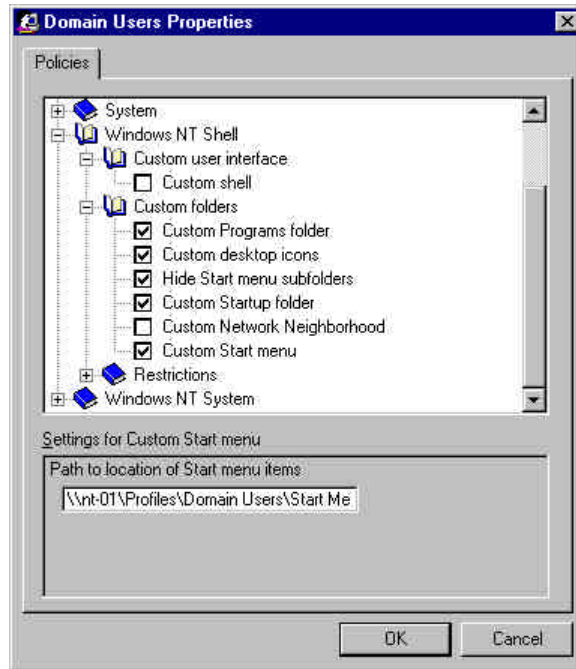
	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
3.	Click the plus box in front of the System icon, then click the plus box in front of the Restrictions item (see Figure 14-10).	<p>Check “Disable Registry editing tools.”</p> <p>Replace the shaded block for “Run only allowed Windows applications” with a solid white block.</p>	<p>Prevents the use of the registry editing tools by an unauthorized user.</p> <p>An additional security measure can be taken by checking “Run only allowed Windows applications.” This allows the Administrator to select which applications a default user can run. This action should be used with extreme caution and by experienced Administrators only.</p>

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
4.	Click the plus box in front of the Windows NT Shell item, then click the plus box in front of the Custom user interface item (see Figure 14-11).	Replace the shaded block with a solid white block on the "Custom Shell" item.	Prevents Domain Users from using a shell other than Explorer.exe.

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
5.	Click the plus box in front of the Windows NT Shell item, then click the plus box in front of the Custom Folders item (see Figure 14-11).	<p>Replace the shaded block with a solid white block on “Custom Network Neighborhood.”</p> <p>Check “Custom Program folder” and enter the following path in the lower dialog box:  “\\&lt;PDC NAME&gt;\Profile\$\Domain Users\Start Menu\Programs.”</p> <p>Check “Custom desktop icons” and enter the following path in the lower dialog box:  “\\&lt;PDC NAME&gt;\Profile\$\Domain Users\Desktop.”</p> <p>Check “Hide Start menu subfolders.”</p> <p>Check “Custom Startup folder” and enter the following path in the lower dialog box:  “\\&lt;PDC NAME&gt;\Profile\$\Domain Users\Start Menu\Programs\Startup.”</p> <p>Check “Custom Start menu” and enter the following path in the lower dialog box:  “\\&lt;PDC NAME&gt;\Profile\$\Domain Users\Start Menu.”</p>	<p>Assigns all Domain Users the same Start menu and desktop environment. This allows ease of maintenance for the Administrator. Programs and/or applications can be granted or revoked from Domain Users by editing one user profile.</p>



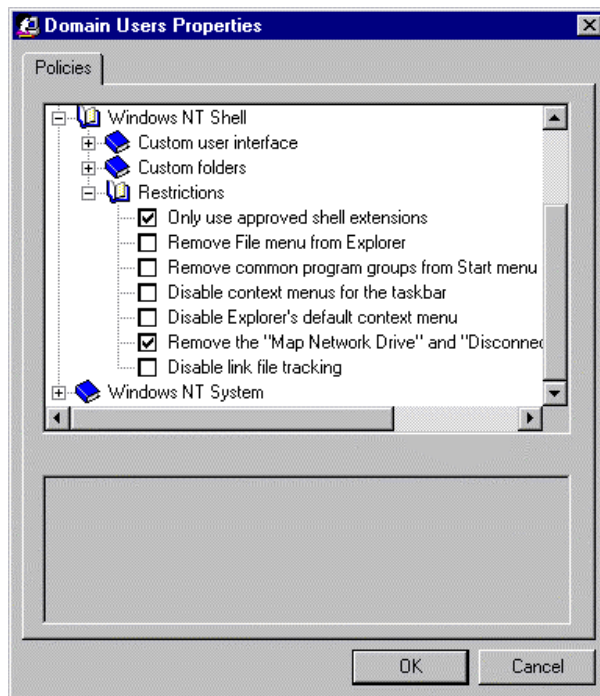
**Figure 14-10. Domain Users Properties - System**



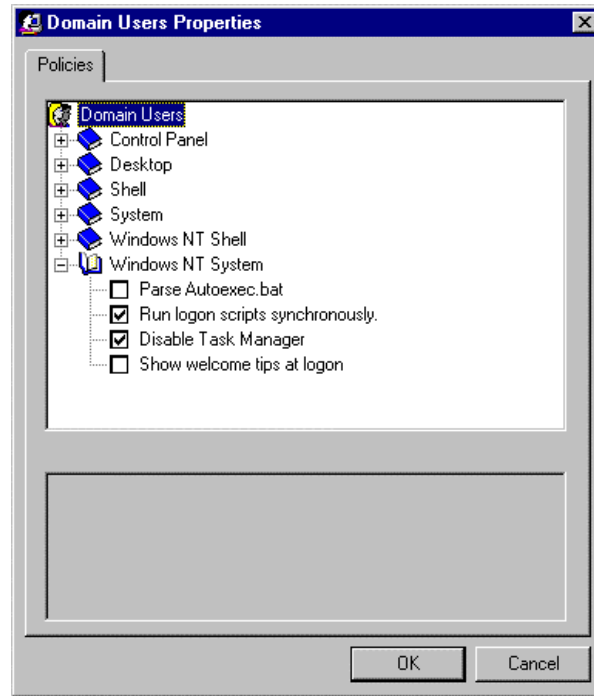
**Figure 14-11. Domain Users Properties - Windows NT Shell/Custom Folders**

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
6.	Click the plus box in front of the Windows NT Shell item, then click the plus box in front of the Restrictions item (see Figure 14-12).	<p>Replace the shaded blocks with solid white blocks on all items except:</p> <p>Check “Only use approved shell extensions”, “Remove the ‘Map Network Drive’ and ‘Disconnect Network Drive’ options.”</p>	Prevents Domain Users from making unauthorized network connections.

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
7.	Click the plus box in front of the Windows NT System item (see Figure 14-13).	<p>Replace the shaded blocks with solid white blocks on the “Parse Autoexec.bat” and “Show welcome tips at logon” items.</p> <p>Check “Run logon scripts synchronously” and “Disable Task Manager.”</p> <p>Click OK.</p>	<p>Performs logon scripts before continuing with the logon process.</p> <p>Prevents Domain Users from starting or stopping system processes and applications through the Task Manager.</p>



**Figure 14-12. Domain Users Properties - Windows NT Shell/Restrictions**



**Figure 14-13. Domain Users Properties - Windows NT System**

Table 14-4 addresses the system policy settings for the Privileged Users group. The procedures only indicate deviations from the system policy settings for the Domain Users group. The Navigate column lists the directions to view and open system windows. The Procedure column lists the options for each step of the configuration. The Rationale column explains the reasoning behind each procedure.

**Table 14-4. Privileged Users Properties**

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
1.	In the System Policy Editor window, single-click on the Domain Users icon.	Select Copy from the Edit menu.	This will copy the properties of the Domain Users policy into memory.

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
2.	Single-click on the Privileged Users icon.	Select Paste from the Edit menu and select Yes.	This will apply the Domain Users policy to the Privileged Users group.
3.	Double-click on the Privileged Users icon. When the Privileged Users Properties window appears, click on the plus box in front of the Control Panel item and click on the plus box in front of the Display item.	Check "Restrict Display", which will make the lower dialog box active. Replace the checked blocks with solid white blocks on all items except "Hide Settings tab."	Prevents Privileged Users from altering the type of display (effects screen resolution, color palette, and monitor type).
4.	Click on the plus box in front of the Shell item, and then click on the plus box in front of the Restrictions item.	Replace the checked blocks with solid white blocks on all selections except:  Keep the "Disable Shutdown command" block grayed-out.	Allows Privileged Users to run executable commands from the Start menu, browse the network outside the domain, and make changes that will impact other users.

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
5.	Click on the plus box in front of the Windows NT Shell item, and then click on the plus box in front of the Custom Folders item.	<p>Check “Custom Program folder” and enter the following path in the lower dialog box:  “\\&lt;PDC NAME&gt;\Profile\$\Privileged Users\Start Menu\Programs.”</p> <p>Check “Custom desktop icons” and enter the following path in the lower dialog box:  “\\&lt;PDC NAME&gt;\Profile\$\Privileged Users\Desktop.”</p> <p>Check “Hide Start menu subfolders.”</p> <p>Check “Custom Startup folder” and enter the following path in the lower dialog box:  “\\&lt;PDC NAME&gt;\Profile\$\Privileged Users\Start Menu\Programs\Startup.”</p> <p>Check “Custom Start menu” and enter the following path in the lower dialog box:  “\\&lt;PDC NAME&gt;\Profile\$\Privileged Users\Start Menu.”</p>	Assigns all Privileged Users the same Start menu and desktop environment. This allows ease of maintenance for the Administrator. Programs and/or applications can be granted or revoked from Privileged Users by editing one user profile.

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
6.	Click the plus box in front of the Windows NT Shell item, then click the plus box in front of the Restrictions item.	Replace the checked block with a solid white block on the “Remove the ‘Map Network Drive’ and ‘Disconnect Network Drive’ options” item.	Allows Privileged Users to create network connections.
7.	Click the plus box in front of the Windows NT System item.	Replace the checked block with a solid white block on the “Disable Task Manager” item. Click OK.	Allows Privileged Users to run the Task Manager.

Table 14-5 addresses the system policy settings for the Domain Admins group. The procedures only indicate deviations from the system policy settings for the Privileged Users group. The Navigate column lists the directions to view and open system windows. The Procedure column lists the options for each step of the configuration. The Rationale column explains the reasoning behind each procedure.

**Table 14-5. Domain Admins Properties**

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
1.	In the System Policy Editor window, single-click on the Privileged Users icon.	Select Copy from the Edit menu.	This will copy the properties of the Privileged Users policy into memory.
2.	Single-click on the Domain Admins icon.	Select Paste from the Edit menu and select Yes.	This will apply the Privileged Users policy to the Domain Admins group.

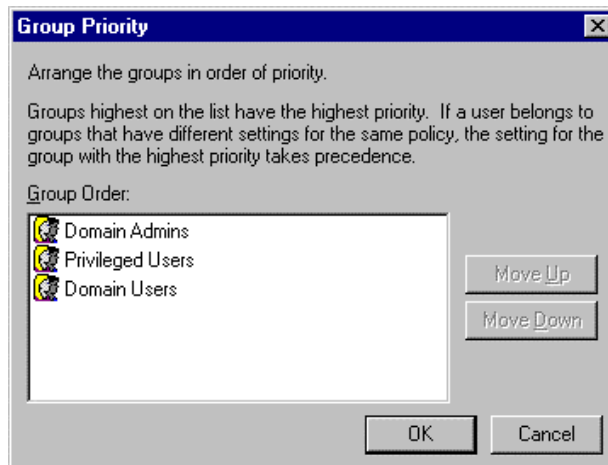
	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
3.	Double-click on the Domain Admins icon. When the Domain Admins Properties window appears, click on the plus box in front of the Control Panel item and click on the plus box in front of the Display item.	Replace the checked block with a solid white block on “Restrict Display.”	Domain Administrators need full control of these settings to address hardware issues.
4.	Click on the plus box in front of the Shell item, and then click on the plus box in front of the Restrictions item.	Replace the checked block with a solid white block on the “Disable Shutdown command” item.	Allows Domain Administrators to shut down the system.
5.	Click on the plus box in front of the System item, and then click on the plus box in front of the Restrictions item.	Replace the checked block with a solid white block on the “Disable Registry editing tools” item.	Allows Domain Administrators to use Registry editing tools to define, delete, and edit Registry settings.

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
6.	Click on the plus box in front of the Windows NT Shell item, and then click on the plus box in front of the Custom Folders item.	<p>Check “Custom Program folder” and enter the following path in the lower dialog box: “\\&lt;PDC NAME&gt;\Profile\Domain Admins\Start Menu\Programs.”</p> <p>Check “Custom desktop icons” and enter the following path in the lower dialog box: “\\&lt;PDC NAME&gt;\Profile\Domain Admins\Desktop.”</p> <p>Check “Hide Start menu subfolders.”</p> <p>Check “Custom Startup folder” and enter the following path in the lower dialog box: “\\&lt;PDC NAME&gt;\Profile\Domain Admins\Start Menu\Programs\Startup.”</p> <p>Check “Custom Start menu” and enter the following path in the lower dialog box: “\\&lt;PDC NAME&gt;\Profile\Domain Admins\Start Menu.”</p> <p>Click OK.</p>	Assigns all Domain Admins the same Start menu and desktop environment. This allows ease of maintenance for the Administrator. Programs and/or applications can be granted or revoked from Domain Admins by editing one user profile.

Table 14-6 lists the steps for saving the system policy settings.

**Table 14-6. Finish With Policy Editor**

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
1.	In the System Policy Editor window, single-click on the Domain Users icon.	Select Copy from the Edit menu.	This will copy the properties of the Domain Users policy into memory.
2.	Single-click on the Default User icon.	Select Paste from the Edit menu.	This will apply the most restrictive policy to a default user.
3.	Select Options from the System Policy Editor menu bar and then select Group Priority.	Ensure that the group order is as follows, from top to bottom (see Figure 14-14):  Domain Admins Privileged Users Domain Users  Click OK.	Ensures the correct (most permissive) policy is loaded for users that are members or more than one group.



**Figure 14-14. System Policy Editor - Group Priority**

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
4.	Without closing the System Policy Editor, open the Server Manager by clicking on the Start button, Run, and then typing “C:\winnt\system32\svrnmgr.exe” in the Run window.	Highlight the Primary Domain Controller by single-clicking on the respective icon. Go to the Computer menu and select Shared Directories. Double-click on the NETLOGON folder. Write down the path so it can be used during the next step to save the system policy that has been created.  Do not close the Server Manager window.	Shows the local path to the NETLOGON directory.
5.	In the System Policy Editor window, select the File menu, then select Save As.	Type “ntconfig.pol” in the file name dialog box and in the upper portion of the Save As window, go to the Netlogon directory. Use the path obtained in step 4. Click Save.	Saves the secure system policy settings.
6.	In the System Policy Editor window, select the File menu.	Select Exit.	Finished with the System Policy Editor.

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
7.	Go to the Server Manager window. All of the machines in the domain should be visible. If not, select All from the View menu (see Figure 14-15).	<p>Select a BDC by clicking on the respective icon.</p> <p>Go to the Computer menu and select Shared Directories. Double-click on the NETLOGON folder. Select Permissions from the “Share Properties” window. In the “Access Through Share Permissions” window select Add. Double-click on the Domain Admins group, and ensure that the name is transferred into the “Add names:” dialog box. Select Change in the “Type of Access” box and click OK.</p> <p>Click OK in the “Access Through Share Permissions” window.</p> <p>Click OK in the “Share Properties” window.</p> <p>Click Close in the “Shared Directories” window.</p>	<p>Each domain controller in the domain must have the same system policy file. This procedure gives Domain Administrators permission to write to the NETLOGON directory of a BDC. This is necessary to distribute the system policy and the permission will be revoked after completing the distribution.</p>

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
8.	Open the Windows NT Explorer. Click the plus box next to Network Neighborhood, and then click on the plus box next to the machine name for your PDC. Double-click on the NETLOGON folder.	Highlight both instances of "ntconfig.pol" by single-clicking on each one while holding down the Control key. Right-click on either file and select Copy.	Copies the files into memory so they can be pasted into the BDC's NETLOGON folders.
9.	In Windows NT Explorer, each BDC should be displayed under Network Neighborhood. Click the plus box next to a BDC.	Right-click on the NETLOGON folder and choose Paste.	Copies the selected files to the correct location on a BDC.
10.	Go to the Server Manager window.	Follow the same procedure in step 5, but in the "Access Through Share Permissions" window, select the Domain Admins group and choose the Remove option.  Click OK in the "Access Through Share Permissions" window.  Click OK in the "Share Properties" window.  Click Close in the "Shared Directories" window.	Revokes the Domain Admins' permission to write to the NETLOGON folder. At the point, the Domain Admins group will be returned to having Read permission to the share.
11.	Continue in the Server Manager window.	Repeat steps 7 through 10 for each BDC in the domain.	Ensures that all BDCs have the same system policy as the PDC.

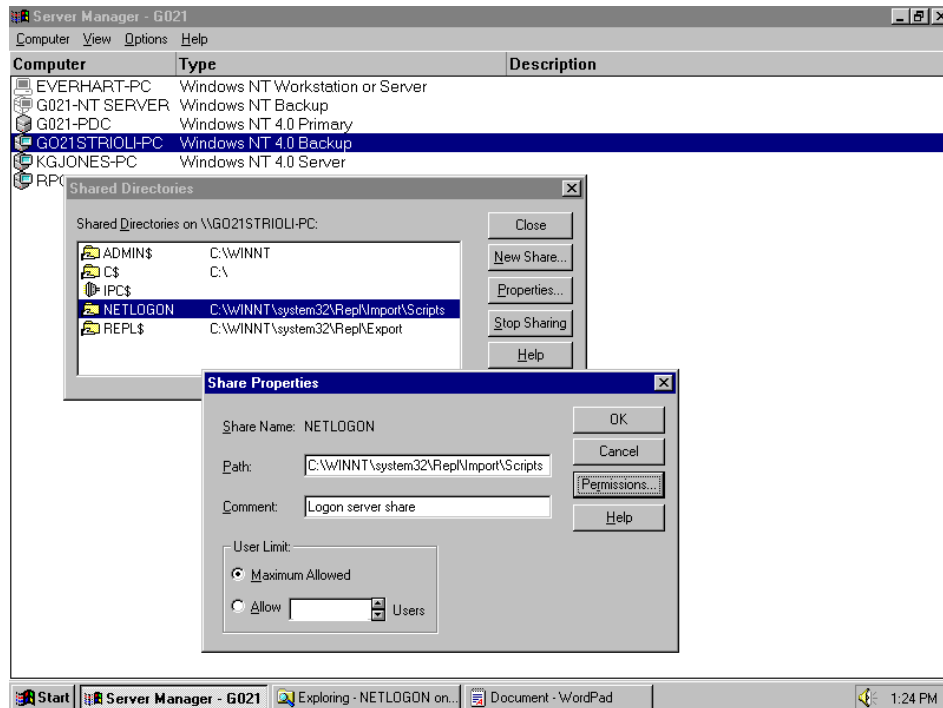


Figure 14-15. Server Manager Window

## Section 15

# Control Panel Configuration

Table 15-1 lists steps for configuring network protocols such as NetBIOS and TCP/IP, general system information, desktop display, printer setup, and services through the Control Panel. These steps should be performed on all servers and workstations in the domain. The Navigate column lists the directions to view and open system windows. The Procedure column lists the options for each step of the configuration. The Rationale column explains the reasoning behind each procedure.

**Table 15-1. Control Panel Configuration Procedures**

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
1.	This step should <b>ONLY</b> be performed on machines with direct connections to the Internet (e.g., gateway machines, routers).  In the Taskbar, click on the Start button, Settings, and then Control Panel. Double-click on the Network icon and then click on the Bindings tab.	Click on NetBIOS Interface and click on the Disable button.  Click the Close button.	Disabling NetBIOS over TCP/IP eliminates the risk of Windows NT networking data and SMB/NetBIOS services being exposed to Internet users.

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
2.	Click on the Protocols tab in the Network window and then double-click on the TCP/IP Protocol entry.	<p>When the TCP/IP Properties window appears (Figure 15-1), do the following:</p> <p>If the appropriate adapter is not listed in the Adapter field, select it from the pull-down menu.</p> <p>Verify the IP addresses in the following three fields: IP Address, Subnet Mask, Default Gateway.</p> <p>Click on the Advanced icon.</p> <p>When the Advanced IP Addressing window appears, ensure that the information in this window is consistent with your selections from the TCP/IP Properties window.</p> <p>Make sure Enable Security is checked and PPTP Filtering is not checked.</p> <p>Click OK twice.</p>	<p>PPTP is not enabled since all participants in the communications path must have routers equipped to handle PPTP for proper operation.</p> <p>Security is enabled and should be configured according to the local system policy concerning allowable ports and protocols.</p>



**Figure 15-1. TCP/IP Properties Box**

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
3.	Continue in the Network window.	Click Close. Do not restart the computer at this time as there are more procedures to do. Click No.	Finished with network configuration.

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
4.	<p>In the Control Panel window, double-click on the System icon.</p> <p>When the System Properties window appears, click on the Startup/Shutdown tab.</p>	<p>Check all five boxes in the Recovery area (When a STOP error occurs):</p> <p>Write an event to the system log, Send an administrative alert *, Write debugging information to, Overwrite any existing file, and Automatically reboot.</p> <p>In the text field following “Write debugging information to:,” enter the pathname and file where the debugging information is to be logged.</p> <p>* Enable this option on servers only</p>	<p>An example pathname to log debugging information is “%systemroot%\MEMORY.DMP.”</p>
5.	<p>In the Systems Properties window, select the Hardware Profiles tab. Click on the Properties button.</p>	<p>When the Original Configuration Properties window appears, do the following:</p> <p>Select the General tab. If the computer is portable, indicate this and select the appropriate fields.</p> <p>Select the Network tab. If the computer is not going to be used for any network applications, check the box “Network-disabled hardware profile.”</p> <p>Click OK.</p>	<p>Configure the hardware setup.</p> <p>NOTE: Selecting “Network-disabled hardware profile” will prevent network card drivers and protocols from being loaded resulting in a standalone machine.</p>

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
6.	Continue in the System Properties window.	Click Apply and then OK. Do not restart the computer at this time as there are more procedures to do. Click No.	Finished with System configuration.
7.	If print capabilities are required from your machine, go to the Control Panel window and double-click on the Printers icon.  Double-click on the Add Printer icon.	In the Add Printer Wizard window, select either My Computer (to have settings managed on your local machine) or Network Printer Server (to have settings managed by the print server). Click Next and fill out the required printer information in each of the subsequent windows.	Consult with your System Administrator for printer setup suitable for your machine.
8.	This step <b>MUST</b> be performed by every user in the domain.  In the Control Panel window, double-click on the Display icon.  When the Display Properties window appears, click on the Screen Saver tab.	Choose a screen saver from the Screen Saver drop-down list. Check the "password protected" option, and then type 15 for "Wait x minutes."  Click Apply and then click OK.	Password-protected logoff screen saver will appear after 15 minutes of inactivity.
9.	Close all application windows. Click on the Start button and select Shut Down.	Select Restart the Computer and click OK.	The computer must be restarted to ensure the new settings will take effect.

## Section 16

# Miscellaneous Configurations

This section includes a list of miscellaneous items to configure or install on your system. The list covers steps to increase password strength, properly limit and disable file shares, disable unnecessary services, and assign appropriate system privileges to groups.

- Increase password strength by utilizing the password filter (“Passfilt.dll”) supplied by Microsoft in Service Pack 3 for Windows NT 4.0. “Passfilt.dll” adds password security by requiring that passwords be at least 6 characters long, may not contain your username/full name, and must contain combinations of uppercase, lowercase, and numeric characters.

This filter will need to be copied to “%systemroot%\system32” after SP3 is installed on the system. To enable the filter, the following registry entry, of type REG\_MULTI\_SZ and value “PASSFILT”, must be configured appropriately:  
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Notification  
Packages

The Notification Packages contains a list of Dynamic Link Libraries (DLLs) to be loaded and notified of password changes and password change requests. If the value “PASSFILT” does not exist in the registry, it must be entered.

NOTE: Notification and filtering only take place on the computer that houses the updated account. Keep this in mind when dealing with domain user accounts. Notification on domain accounts only takes place on the PDC. Notification packages should be installed on all BDCs in a domain, in addition to the PDC, to allow notifications to continue in the event of server role changes.

- Use the “passprop.exe” utility in the Windows NT Server Resource Kit to display or modify domain policies for password complexity and Administrator lockout. Enter the following command in the Run window to display more details on the options available for the PASSPROP command:

```
PASSPROP /?
```

To configure the Administrator’s password properties, enter the following command in the Run window:

```
PASSPROP /complex /adminlockout
```

The option /complex forces passwords to be complex, requiring passwords to be a mix of upper and lowercase letters and numbers or symbols.

The option /adminlockout allows the Administrator account to be locked out. The Administrator account can still log on interactively on domain controllers.

- Substitute the Authenticated Users group to bypass the Everyone group for many objects (e.g., files, directories, registry keys). Assign the same permissions previously held by the Everyone group to the Authenticated Users group.
- Disable all FTP services on Windows NT servers (if it is not required) and any other unnecessary services including PPTP, NetBEUI, RAS, and NWLink.
- Increase the level of encryption on the account password information stored in the registry by the Security Account Manager (SAM) by using Syskey.exe from SP3:
  - From the Start Menu, choose Run and enter the following command in the dialog box: "C:\winnt\system32\syskey.exe."
  - Choose Encryption enabled and click OK. NOTE: After encryption is enabled, it cannot be disabled.
  - Create an emergency repair disk with the new encrypted portion of the SAM using the "rdisk /s" procedure outlined in steps 4 and 5 of Table 5-1. Label this disk "ERD – Post SAM Encryption" or something similar.
- Protect all Windows NT nodes with direct access to the Internet (e.g., gateway machines or routers) by performing the following configuration changes:
  - Stop or unbind the Server service, so that no shares will be available from this node.
  - Disable NetBIOS over TCP/IP through the Bindings tab in the Control Panel.

The items listed below are useful tips:

- Remove any file shares on directories before deleting the directory itself. If a directory which contains a file share is simply deleted before removing the share, another directory created in the future with the same name will inherit the same share settings.
- Many attacks against Windows NT are successful when they take place at the console. These attacks require the system to be powered down and booted from a floppy disk. Utilities such as NTFSDOS allow a machine that has been booted from a DOS floppy disk to read an NTFS partition and thus compromise critical information. A few measures can be taken to circumvent such an attack:
  - The first step is to enter the setup program (also known as BIOS or CMOS) on a machine (usually a key sequence is entered during the initial boot process of a machine). In the setup options, there will be a setting to disable booting from the floppy disk drive.
  - To secure this change, the second step requires setting a password on accessing the setup program. This is an easy setting to configure in the setup options.

- The final step is to save these settings and to exit the setup program.

## Section 17

# System Repair Data

This section contains procedures for ensuring that the system repair data is properly backed up and secured. If this is a new installation and the Emergency Repair Disk has just been created, the System Administrator can skip this section as the data is up to date. For a computer that has not been recently configured, continue with this section.

System repair data is stored in two places by the Windows NT operating system. The first place is on the ERD floppy disk. This disk should have been created during the original system installation and then repeated at certain time intervals. The system repair data utility should be run after any of the following events have occurred:

- Installation of a Service Pack (e.g., SP3)
- Installation of any application
- Disk conversion to NTFS (using the “convert.exe” utility)
- Volume set configuration (from Disk Administrator)
- Stripe set configuration (from Disk Administrator)
- Addition of a large number of user accounts

The second place in which system repair data is stored is in the “%systemroot%\repair” directory. The procedures listed in Table 17-1 ensure that the ERD is up to date, its data is properly protected, and repair data stored on the hard drive is protected. These steps should be performed on all servers and workstations in the domain. The Navigate column lists the directions to view and open system windows. The Procedure column lists the options for each step of the configuration. The Rationale column explains the reasoning behind each procedure.

**Table 17-1. System Repair Procedures**

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
1.	Find the Emergency Repair Disk for the particular machine.	Ensure that the floppy disk is physically write protected and it's date of creation is reasonable.  If the floppy disk needs to be updated (creation date is old), proceed to the next step.  If the ERD cannot be located, proceed to step 3.	It is imperative that the data on the ERD is up to date and is securely stored. The ERD contains SAM information and should be physically protected (e.g., stored in a safe or locked cabinet).
2.	In the Taskbar, click on the Start button, Programs, and then select Windows NT Explorer.  When the Exploring window appears, click the View menu, and then the Details item.  Use the Exploring window to find the "%systemroot%\repair" directory.	If the creation dates of the files are reasonable, skip the next two steps.	Ensure that the data is protected and reflects the current state of the system.
3.	In the Taskbar, click on the Start button and then select Run.	When the Run window appears (Figure 17-1), type "rdisk /s" and then click the OK button.	Updates the system repair data with the latest configuration information.
4.	When the rdisk utility finishes saving the current system information, a Setup window will appear.	Click Yes to create the ERD. Insert the floppy disk and click OK.  Store the ERD in a safe or locked cabinet.	Creates an upgraded copy of the ERD.

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
5.	From the previous Exploring window, select the “%systemroot%\ repair” directory, right-click on each file, select Properties, click the Security tab, and then select the Permissions button.	For each file, ensure that the following permissions are set: <b>Administrators</b> Full Control <b>SYSTEM</b> Full Control	The files in this directory must be protected because they contain configuration information for effective recovery in the event of a system failure.



**Figure 17-1. Run Window**

The procedures in Table 17-2 ensure the utility that creates system repair data (“rdisk”) is properly protected. These steps should be performed on all servers and workstations in the domain. The Navigate column lists the directions to view and open system windows. The Procedure column lists the options for each step of the configuration. The Rationale column explains the reasoning behind each procedure.

**Table 17-2. “Rdisk” Permissions**

	<b>Navigate</b>	<b>Procedure</b>	<b>Rationale</b>
1.	<p>In the Taskbar, click on the Start button, Programs, and then select Windows NT Explorer.</p> <p>When the Exploring window appears, find the “%systemroot%\system32” directory, right-click on the “rdisk.exe” file, and select Properties.</p> <p>When the “rdisk” Properties window appears, click on the Security tab and then click the Permissions button.</p>	<p>When the File Permissions window appears, ensure that the following rights are set:</p> <p><b>Administrators</b> Full Control</p> <p><b>Server Operators *</b> Change</p> <p><b>System</b> Full Control</p> <p>Remove the Everyone group if it appears in the window.</p> <p>* Applies to servers only.</p>	<p>Limiting access to the system repair disk backup utility ensures that vital data will not be inadvertently overwritten.</p>

## Bibliography

This bibliography is divided into the following four parts: Uniform Resource Locators (URLs), books, manuals, and reports.

### URLs

Archives of the NT Security discussion list: <ftp://ftp.iss.net/pub/lists/ntsecurity-digest.archive>

NT Security, Frequently Asked Questions: <http://www.it.kth.se/~rom/ntsec.html>

Somarsoft's Windows NT Security Issues: <http://www.somarsoft.com/security.htm>

On-line books by Charles Rutstein entitled *Windows NT Security*:

<http://www.betabooks.mcgraw-hill.com/rutstein/>,

<http://ourworld.compuserve.com/homepages/cbr/toc.htm>, <http://www.ntresearch.com/>

Security Issues of an NT Web Server: <http://www.telemark.net/~randallg/ntsecure.htm>,

<http://www.ntsecurity.com/index.htm>

Sunbelt Software NT system utilities: <http://www.ntsoftdist.com/>

Defense Information Infrastructure Common Operating Environment (DII COE) Version 3.1

Consolidated Documents for NT 4.0: [http://spider.osfl.disa.mil/cm/cm\\_page.html](http://spider.osfl.disa.mil/cm/cm_page.html)

Intrusion Detection, Inc., specializes in Novell, Windows NT, and general network security, product development, and security consulting: <http://www.intrusion.com/>

### Books

Citibank, Coopers & Lybrand, The Institute of Internal Auditors, and Microsoft, *Windows NT Guidelines for Security, Audit, and Control*, 1994, Microsoft Press.

Jennings, R., 1997, *Using Windows NT Server 4*, Que Corporation.

Minasi, Anderson, and Creegan, January 1996, *Mastering Windows NT Server 4*, Sybex.

Rutstein, C., 1997, *Windows NT Security: A Practical Guide to Securing Windows NT Servers and Workstations*, Computing McGraw-Hill.

Sheldon, T., 1997, *The Windows NT Security Handbook*, Osborne McGraw-Hill.

Siyam, K., January 1997, *Windows NT Server Professional Reference*, New Riders Publishing.

Sutton, S., 1997, *Windows NT Security*, Addison Wesley Developers Press.

## **Manuals**

*Concepts and Planning Microsoft Windows NT Server Version 4.0*, 1996, Microsoft Corporation, Document No. 69940-0696.

*Start Here Basics and Installation Microsoft Windows NT Server Version 4.0*, 1996, Microsoft Corporation, Document No. 69935-0696.

*Start Here Basics and Installation Microsoft Windows NT Workstation Version 4.0*, 1996, Microsoft Corporation, Document No. 69396-0696.

## **Reports**

Department of Defense, 1985, *Trusted Computer System Evaluation Criteria*, DOD 5200.28-STD, Washington, D.C.

E-mail message, "Information Technology for the 21<sup>st</sup> Century," March 1997, Navy Administrative message, CINCPACFLT, Pearl Harbor, HI.

## Appendix A

# Hotfixes

Hotfixes are supplied by Microsoft for updating the Windows NT operating system since the release of the latest Service Pack (SP). Since hotfixes are published after solutions have been developed for system problems, it is imperative for System Administrators to be aware of newly released hotfixes. Hotfixes are not cumulative and therefore must be installed in sequential order after the latest Service Pack has been applied.

Hotfixes are typically contained as self-extracting files which may be downloaded from Microsoft's FTP site at: <ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3>. For Intel-based machines, the appropriate filenames end with ".i.exe." For example, "lsa-fixi.exe" is the LSA hotfix for an Intel-based machine. Each hotfix is stored in a directory containing the executable hotfix, a "readme.txt" file that explains how to apply the hotfix, and a "Q<number>.txt" file, where <number> is the index into Microsoft's Knowledge Base. The Knowledge Base describes the cause and resolution of the problem and can be accessed at Microsoft's web site.

Table A-1 lists the hotfixes (in chronological order) that can be applied to every server and workstation in the domain. The Hotfix column lists the names of each hotfix. The Date column lists the release date of the hotfix. The URL column lists the URL where each hotfix can be downloaded from Microsoft's web site. Mandatory hotfixes are indicated by a "\*" next to their name and MUST be applied to every machine in the domain. Optional hotfixes do not have a "\*" by their name and should only be applied if the particular machine is impacted by the problem addressed in the hotfix.

The following steps define the procedure for installing a hotfix:

1. Ensure that all hotfixes are stored within separate directories.
2. Open a command-prompt window and change to a hotfix directory.
3. Extract the contents of the hotfix by running the hotfix executable file with the -x switch (e.g., `getadmin-fixi.exe -x`).
4. Apply the hotfix by running the hotfix executable file without switches (e.g., `getadmin-fixi.exe`).
5. Reboot the machine by clicking OK in the dialog box that appears after the hotfix is installed.

Hotfixes must be reinstalled after additional software is added to the system to ensure that the proper version of the DLLs is present on the system. Microsoft does not perform complete regression testing of hotfixes against all applications, therefore it is the responsibility

of the individual to ensure that the hotfixes do not disrupt the proper operation of the applications.

To uninstall a hotfix, use the following procedures:

1. Open a command-prompt window and change to the directory of the hotfix that is to be uninstalled.
2. Uninstall the hotfix by issuing the following command: hotfix.exe -y -z. The “-y” switch is for uninstallation and the “-z” switch will stop the machine from rebooting after the uninstallation.
3. Uninstall any additional hotfixes using the same method.
4. Reboot the machine.

**This list of hotfixes is current as of December 4, 1998.** The Microsoft FTP site should be checked frequently for updates and additions of hotfixes.

**Table A-1. Hotfixes**

<b>Hotfix</b>	<b>Date</b>	<b>URL</b>
asp-fix	May 22, 1997	ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/asp-fix
iis-fix	June 21, 1997	ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/iis-fix
Winsupd-fix *	August 8, 1997	ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/winsupd-fix
ndis-fix *	August 11, 1997	ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/ndis-fix
dns-fix	August 13, 1997	ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/dns-fix
getadmin-fix *	August 27, 1997	ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/getadmin-fix
scsi-fix	September 8, 1997	ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/scsi-fix
simptcp-fix *	November 3, 1997	ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/simptcp-fix
2gcrash	November 3,	ftp://ftp.microsoft.com/bussys/winnt/winnt-

<b>Hotfix</b>	<b>Date</b>	<b>URL</b>
	1997	public/fixes/usa/nt40/hotfixes-postSP3/2gcrash
ide-fix	November 19, 1997	ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/ide-fix
wan-fix	November 20, 1997	ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/wan-fix
joystick-fix	December 11, 1997	ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/joystick-fix
iis4-fix	December 12, 1997	ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/iis4-fix
roll-up	December 12, 1997	ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/roll-up
SAG-fix	December 17, 1997	ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/SAG-fix
teardrop2-fix *	January 12, 1998	ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/teardrop2-fix
tapi21-fix	January 22, 1998	ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/tapi21-fix
zip-fix	February 12, 1998	ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/zip-fix
srv-fix *	February 13, 1998	ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/srv-fix
pcm-fix	February 16, 1998	ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/pcm-fix
pent-fix *	March 5, 1998	ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/pent-fix
Y2k-fix *	April 8, 1998	ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/y2k-fix
Atapi-fix	April 16, 1998	ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/atapi-fix
Netbt-fix *	April 23, 1998	ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/netbt-fix

Hotfix	Date	URL
Prnt-fix *	May 7, 1998	ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/prnt-fix
Sfm-fix	June 3, 1998	ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/sfm-fix
Ssl-fix	July 17, 1998	ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/ssl-fix
Lsa2-fix *	July 20, 1998	ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/lsa2-fix
Priv-fix *	July 28, 1998	ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/priv-fix
Rras30-fix	August 18, 1998	ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/rras30-fix
Pptp3-fix	August 18, 1998	ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/pptp3-fix
Snk-fix *	September 30, 1998	ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/snk-fix

The following list provides a brief summary of each mandatory (and optional) hotfix:

- **ASP-fix.** This hotfix corrects a memory leak in Microsoft Active Server Pages version 1.0B (as part of Microsoft Internet Information Server, version 3.0) which may cause performance problems. For more information, refer to the following article in the Microsoft Knowledge Base: Q165335.
- **Atapi-fix.** This hotfix fixes the problem with Windows NT incorrectly reporting the size of a 10.1-gigabytes (GB) capacity IBM DTTA-351010 fixed disk drive to be 7,550 megabytes (7.5 GB) even though the System BIOS supports INT 13 extensions and can see the full capacity of the drive. For more information, refer to the following article in the Microsoft Knowledge Base: Q183654.
- **DNS-fix.** This hotfix solves a number of different problems associated with the DNS server. This hotfix is not dependent on SP3. For more information, refer to the following articles in the Microsoft Knowledge Base: Q142047, Q154984, Q154985, Q167629, and Q169461.
- **Getadmin-fix.** This hotfix prevents a user from obtaining Administrative rights. This hotfix also includes fixes for Java Applets and double-clicking the mouse

button. Do not apply the dblclick-fix or java-fix after applying this fix. For more information, refer to the following articles in the Microsoft Knowledge Base: Q146965, Q168748, and Q170510.

- **IDE-fix.** Computers that support shut down and power down features may have their power turned off before the write cache is flushed. For more information, refer to the following article in the Microsoft Knowledge Base: Q153296.
- **IIS-fix.** This hotfix corrects the problem associated with the Internet Information Server stopping when it receives a HTTP GET packet from a browser that contains between four and eight kilobytes of data in the URL. For more information, refer to the following article in the Microsoft Knowledge Base: Q143484.
- **IIS4-fix.** This hotfix corrects the problem with the timewait state queue management causing wait states to exceed four minutes under stress. For more information, refer to the following article in the Microsoft Knowledge Base: Q169274.
- **Joystick-fix.** The value of the calibration bar may not change when you attempt to calibrate foot pedals attached to the joystick game port. For more information, refer to the following article in the Microsoft Knowledge Base: Q177668.
- **Lsa2-fix.** This hotfix prevents against Administrators from using APIs published in the Win32 SDK to display contents of security information stored by the Local Security Authority (LSA) in a form called LSA Secrets. The hotfix also enables logging of failed domain logon attempts to appear in the domain controller's event logs. For more information, refer to the following articles in the Microsoft Knowledge Base: Q184017, Q182918.
- **NDIS-fix.** This hotfix corrects the problem when intermediate Network Driver Interface Specification (NDIS) miniport drivers are used. Intermediate drivers are typically add-ons that layer themselves over hardware drivers to provide additional functionality. The symptoms may either be a memory leak or a blue screen STOP message, indicating that a bad instruction has been executed in the "Ndis.sys" driver. For more information, refer to the following article in the Microsoft Knowledge Base: Q156655.
- **Netbt-fix.** This hotfix corrects the problem with Windows NT waiting for a connection attempt over a local LAN to timeout before the connection over RAS is accepted. For more information, refer to the following article in the Microsoft Knowledge Base: Q178205.
- **Pcm-fix.** This hotfix corrects the problem when the Xircom CBE-10/100BTX PC card fails to function due to the PC card driver resetting the type field when the

card is initialized. For more information, refer to the following article in the Microsoft Knowledge Base: Q180532.

- **Pent-fix.** When an Intel processor receives a specific invalid instruction, the computer may stop responding (hang). The computer must then be turned off and restarted to return to normal operation. For more information, refer to the following article in the Microsoft Knowledge Base: Q163852.
- **Pptp3-fix.** This hotfix contains the Point to Point Tunneling Protocol (PPTP) Performance Update for Microsoft Windows NT server and workstation. For more information, refer to the following article in the Microsoft Knowledge Base: Q189595.
- **Priv-fix.** This hotfix prevents against the Sechole.exe utility, which can allow a non-administrative user to gain debug-level access on a system process, and therefore run code in a security context to give themselves Administrative privileges on the system. For more information, refer to the following article in the Microsoft Knowledge Base: Q190288.
- **Prnt-fix.** This hotfix corrects the problem of a local port monitor resetting faster than the port can become ready when attempting to print to a parallel port on a Windows NT machine. For more information, refer to the following article in the Microsoft Knowledge Base: Q181022.
- **Roll-up.** This hotfix corrects the problem when an access violation occurs in Windows NT Explorer and other applications while running Microsoft Transaction Server (MTS). For more information, refer to the following article in the Microsoft Knowledge Base: Q147222.
- **Rras30-fix.** This hotfix contains the Routing and Remote Access upgrade for Microsoft Windows NT 4.0 Server Hotfix Pack 2.0. For more information, refer to the following article in the Microsoft Knowledge Base: Q189594.
- **SAG-fix.** A Windows NT client or server that receives EBCDIC characters from an IBM-compatible computer does not convert properly from EBCDIC character codes to ANSI character codes. For more information, refer to the following article in the Microsoft Knowledge Base: Q177471.
- **SCSI-fix.** This hotfix corrects the problem with the CLARiON Trespass utility. For more information, refer to the following article in the Microsoft Knowledge Base: Q171295.
- **Sfm-fix.** This hotfix corrects various problems with a Windows NT machine (running Services for Macintosh) encountering STOP errors, incorrect file time/date stamps, and files shifting when accessed by Macintosh clients. For more information, refer to the following articles in the Microsoft Knowledge Base:

Q166571, Q170965, Q172511, Q177644, Q178364, Q180622, Q180716, Q180717, Q180718, Q185722.

- **SimpTCP-fix.** This hotfix guards against an attack consisting of a flood of UDP datagrams sent to the subnet broadcast address with the destination port set to 19 (Character Generator port) and a spoofed source IP address. For more information, refer to the following article in the Microsoft Knowledge Base: Q154460.
- **Snk-fix.** This hotfix fixes problems with system and network performance degrading and the Rpcss.exe process using 100 percent of CPU time. These problems may occur due to an RPC spoofing attack. For more information, refer to the following article in the Microsoft Knowledge Base: Q193233.
- **Ssl-fix.** This hotfix contains an updated version of the schannel.dll file which resolves a vulnerability in SSL. For more information, refer to the following article in the Microsoft Knowledge Base: Q148427.
- **Srv-fix.** This hotfix prevents against a denial of service attack that causes Windows NT systems to reboot. Due to incorrect processing of the SMB logon packet, memory corruption occurs within the Windows NT kernel. As a result of the memory corruption, a "Blue Screen" occurs, and the system reboots, and in some instances hangs on this screen. For more information, refer to the following article in the Microsoft Knowledge Base: Q180963.
- **Tapi21-fix.** This hotfix corrects various problems when using TAPI 2.1. For more information, refer to the following article in the Microsoft Knowledge Base: Q179187.
- **Teardrop2-fix.** This hotfix corrects the problem when Windows NT stops responding with a STOP 0x0000000A or 0x00000019 message after receiving a number of deliberately corrupted UDP packets. This hotfix incorporates the former Icmp-fix and land-fix from Microsoft. For more information, refer to the following article in the Microsoft Knowledge Base: Q179129.
- **Wan-fix.** This hotfix corrects the problem when a STOP 0x0000000A on a Windows NT computer occurs when copying files via RAS over a SLIP (Serial Line Interface Protocol) connection. For more information, refer to the following article in the Microsoft Knowledge Base: Q163251.
- **WINSupd-fix.** This hotfix corrects the problem with the WINS terminating when it receives an invalid UDP frame. For more information, refer to the following article in the Microsoft Knowledge Base: Q155701.
- **Y2k-fix.** This hotfix corrects problems with User Manager and Windows Explorer recognizing the year 2000. For more information, refer to the following articles in the Microsoft Knowledge Base: Q175093, Q180122, Q180123, Q183125.

- **ZIP-fix.** This hotfix corrects the problem of not being able to access the disk in the ATAPI version of an Iomega Zip drive. For more information, refer to the following article in the Microsoft Knowledge Base: Q154094.
- **2gcrash.** This hotfix corrects the problem with large Memory.dmp file images being produced and the need for support utilities to be updated to read these Memory.dmp images. For more information, refer to the following article in the Microsoft Knowledge Base: Q173277.

## Appendix B

# Administrative Checklist

Certain actions should be performed by an Administrator on a regular basis to maintain the security in their Windows NT domain. Table B-1 lists actions that should be performed along with a recommended frequency. The purpose of this list is to serve as a reminder for Administrators to maintain the security configurations, policies, users, and data of their domain.

**Table B-1. Administrative Checklist**

Action	Frequency
Review audit logs in the Windows NT Event Viewer	Local policy issue based on size of logs and amount of audit data. Refer to Section 7.
Archive audit data	Local policy issues based on size of logs and amount of data. Refer to Section 7 for steps to archive audit data.
Back up data on file servers/workstations (user data)	Local policy issue
Update Emergency Repair Disks and store them in a safe location	ERDs should be updated after performing installations of Service Packs, applications, or hotfixes, disk conversions to NTFS, volume set configuration, stripe set configuration, registry changes, or after adding a large number of users. Refer to Section 17.
Reset passwords as needed	Passwords should be reset before expiration, specifically for accounts created for applications (e.g., Microsoft Exchange). Refer to Section 10 for password policy information.
Install current hotfixes and Service Packs from Microsoft	Hotfixes listed in this guide are dated as of February 17, 1998. Refer to Appendix A for descriptions and to Microsoft's ftp site for the latest available hotfixes: <a href="ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3">ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3</a>

<b>Action</b>	<b>Frequency</b>
Sync the system time with PDC	Local policy issue.
Review and apply permissions to new shares, directories, and files created	Permissions should be applied to all new shares, directories, files, and executables placed on machines in the domain. Refer to Section 6 for recommended file system permissions.
Review current trust relationships	Local policy issue. Refer to Section 12 for creating and removing trust relationships.
Review all user groups and verify the members are valid users and have appropriate rights	User groups should be checked after new users are created in the domain to ensure they have proper group memberships. Refer to Section 9 for creating users and groups through the User Manager for Domains tool.
Review current system policies and apply to new groups	System policies should be periodically checked to ensure all new groups have an appropriate policy. Refer to Section 14 for system policy configuration information.

# Glossary

<b>ACL</b>	Access Control List
<b>AIS</b>	automated information system
<b>AUTODIN</b>	Automatic Digital Network
<b>BDC</b>	Backup Domain Controller
<b>C4I</b>	command, control, communications, computers, and intelligence
<b>CD</b>	compact disk
<b>CD-ROM</b>	compact disk read-only memory
<b>COTS</b>	commercial off-the-shelf
<b>CPU</b>	central processing unit
<b>DAC</b>	discretionary access control
<b>DHCP</b>	Dynamic Host Configuration Protocol
<b>DII COE</b>	Defense Information Infrastructure Common Operating Environment
<b>DLL</b>	Dynamic Link Library
<b>DNS</b>	Domain Name Service
<b>DOD</b>	Department of Defense
<b>ERD</b>	Emergency Repair Disk
<b>GB</b>	gigabyte
<b>GOTS</b>	Government off-the-shelf
<b>IIS</b>	Internet Information Server
<b>INFOSEC</b>	Information Security
<b>JTA</b>	Joint Technical Architecture
<b>K</b>	thousand
<b>LAN</b>	local area network
<b>MB</b>	megabyte
<b>MHz</b>	megahertz
<b>MS-DOS</b>	Microsoft Disk Operating System
<b>NetBEUI</b>	NetBIOS Extended User Interface
<b>NOS</b>	network operating systems
<b>NTFS</b>	NT File System
<b>NTS</b>	Windows NT Server
<b>NTW</b>	Windows NT Workstation
<b>ODBC</b>	Open Database Connectivity
<b>OS</b>	operating systems
<b>PDC</b>	Primary Domain Controller
<b>PMO</b>	Program Management Office
<b>POSIX</b>	Portable Operating System Interface
<b>PPTP</b>	Point-to-Point Tunneling Protocol

<b>RAM</b>	Random Access Memory
<b>RAS</b>	Remote Access Service
<b>RISC</b>	Reduced Instruction Set Computer
<b>SPAWAR</b>	Space and Naval Warfare Systems Command
<b>SP3</b>	Service Pack 3
<b>SQL</b>	Structured Query Language
<b>TCP/IP</b>	Transmission Control Protocol/Internet Protocol
<b>UDP</b>	User Datagram Protocol
<b>UID</b>	User Identifier
<b>UPS</b>	uninterruptable power source
<b>URL</b>	Uniform Resource Locator
<b>VGA</b>	Video Graphics Adapter
<b>WINS</b>	Windows Internet Naming Service

# Distribution List

## Internal

### G021

A. J. Jackman  
R. P. Galloni  
J. F. Otin

### G023

T. A. Gregg  
C. R. Oakes  
C. L. Pratt  
R. C. Reopell  
L. M. Sosnosky  
G023 Files (2)

### Records Resources (3)

## External

Commander, Space and Warfare Systems  
Command  
53560 Hull Street  
San Diego, CA 92152-5002

CAPT D. Galik, SPAWAR PMW 161A  
Mr. S. Henderson, SPAWAR PMW 161E  
Mr. M. Hunter, SPAWAR PMW 161  
Mr. S. McCardle, SPAWAR PMW 161  
Mr. M. Morey, SPAWAR PMW 161  
Mr. P. Moylan, SPAWAR PMW 161  
Mr. F. Ottaviano, SPAWAR PMW 161  
Mr. J. Patterson, SPAWAR PMW 161  
Mr. J. Stawiski, SPAWAR PMW 161  
Mr. D. Terhune, SPAWAR PMW 161

Naval Research Laboratory

4555 Overlook Avenue SW  
Washington, DC 20375-5000

Mr. D. Mihelcic, NRL

DISA Counterdrug Integration Division, Code  
D64  
701 S. Courthouse Road (D64 at Skyline 5,  
Suite 105)  
Arlington, VA 22204-2199

Mr. R. Parker

Office of Naval Intelligence  
JDISS  
4251 Suitland Road  
Washington, DC 20395

Mr. W. Essex



