

# Microsoft Windows NT

---

## Securing Windows NT Installation

October 23, 1997

Microsoft Corporation

### Contents

#### Abstract

#### Establishing Computer Security

- Levels of Security
- Off-the-Shelf vs. Custom Software
- Minimal Security
- Standard Security
- High-Level Security

#### High-Level Software Security Considerations

- User Rights
- Protecting Files and Directories
- Protecting the Registry
- Secure EventLog Viewing
- Secure Print Driver Installation
- The Schedule Service (AT Command)
- Secure File Sharing
- FTP Service
- NetBios Access From Internet
- Hiding the Last User Name
- Restricting the Boot Process
- Allowing Only Logged-On Users to Shut Down the Computer
- Controlling Access to Removable Media
- Securing Base System Objects
- Enabling System Auditing
- Enhanced Protection for Security Accounts Manager Database
- Restricting Anonymous network access to Registry
- Restricting Anonymous network access to lookup account names and groups and network shares
- Enforcing strong user passwords
- Disabling LanManager Password Hash Support
- Wiping the System Page File during clean system shutdown
- Disable Caching of Logon Credentials during interactive logon.

#### C2 Security

- Evaluation vs. Certification
- Setting up a C2-compliant System

## **Abstract**

Microsoft® Windows NT® operating system provides a rich set of security features. However, the default out-of-the-box configuration is highly relaxed, especially on the Workstation product. This is because the operating system is sold as a shrink-wrapped product with an assumption that an average customer may not want to worry about a highly restrained but secure system on their desktop. This assumption has changed over the years as Windows NT gains popularity largely because of its security features. Microsoft is investigating a better secured default configuration for future releases. In the meantime, this white paper talks about various security issues with respect to configuring all Windows NT version 4.0 OS products for a highly secure computing environment.

The paper is intentionally kept informational with few recommendations. A particular installation's requirements can differ significantly from another. Therefore, it is necessary for individual customers to evaluate their particular environment and requirements before implementing a security configuration. This is also because implementing security settings can impact system configuration. Certain applications installed on Windows NT may require more relaxed settings to function properly than others because of the nature of the product. Customers are therefore advised to carefully evaluate recommendations in the context of their system configurations and usage.

**Note:** The Microsoft Desktop and Business Systems Division series of white papers is designed to educate information technology (IT) professionals about Windows NT and the Microsoft BackOffice family of products. While current technologies used in Microsoft products are often covered, the real purpose of these papers is to give readers an idea of how major technologies are evolving, how Microsoft is using those technologies, and how this information affects technology planners.

For the latest information on Windows NT Server, check out our World Wide Web site at <http://www.microsoft.com/backoffice/> or the Windows NT Server Forum on the Microsoft Network (GO WORD: MSNTS).

**Note:** The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

## **Establishing Computer Security**

### **Levels of Security**

Windows NT allows you to establish a full range of levels of security, from no security at all to the C2 level of security required by many government agencies. In this chapter, we describe three levels of security—minimal, standard, and high-level—and the options used to provide each level. These levels are arbitrary, and you will probably want to create your own “level” by blending characteristics of the levels presented here.

Why not have maximum security at all times? One reason is that the limits you set on access to computer resources make it a little harder for people to work with the protected resources. Another is that it is extra work to set up and maintain the protections you want. For example, if only users who are members of the HR user group are allowed to access employee records, and a new person is hired to do that job, then someone needs to set up an account for the new hire and add that account to the HR group. If the new account is created but not added to HR, the new hire cannot access the employee records and therefore cannot perform his or her job.

If the security is too tight, users will try to circumvent security in order to get work done. For example, if you set the password policy such that passwords are hard to remember, users will write them down to avoid being locked out. If some users are blocked from files they need to use, their colleagues might share their own passwords in order to promote the flow of work.

The first step in establishing security is to make an accurate assessment of your needs. Then choose the elements of security that you want, and implement them. Make sure your users know what they need to do to maintain security, and why it is important. Finally, monitor your system and make adjustments as needed.

## **Off-the-Shelf vs. Custom Software**

If you are using software made especially for your installation, or if you are using shareware that you aren't sure you can trust, and you want to maintain fairly high security, it is recommended that you look at Appendix B of the *Microsoft® Windows NT® Workstation Resource Guide*, “Security In a Software Development Environment.” This provides information on settings and calls that can support—or circumvent—security settings.

## **Minimal Security**

You might not be concerned with security if the computer is not used to store or access sensitive data or if it is in a very secure location. For example, if the computer is in the home office of a sole proprietor of a business, or if it is used as a test machine in the locked lab of a software development company, then security precautions might be unnecessarily cumbersome. Windows NT allows you to make the system fully accessible, with no protections at all, if that is what your setup requires.

## **Physical Security Considerations**

Take the precautions you would with any piece of valuable equipment to protect against casual theft. This step can include locking the room the computer is in when no one is

there to keep an eye on it, or using a locked cable to attach the unit to a wall. You might also want to establish procedures for moving or repairing the computer so that the computer or its components cannot be taken under false pretenses.

Use a surge protector or power conditioner to protect the computer and its peripherals from power spikes. Also, perform regular disk scans and defragmentation to isolate bad sectors and to maintain the highest possible disk performance.

### **Minimal Software Security Considerations**

For minimal security, none of the Windows NT security features are used. In fact, you can allow automatic log on to the Administrator account (or any other user account) by following the directions in Chapter 25 “Configuration Management and the Registry” in *Windows NT Workstation Resource Guide*. This allows anyone with physical access to the computer to turn it on and immediately have full access to the computer’s resources.

By default, access is limited to certain files. For minimal security, give the Everyone group full access to all files.

You should still take precautions against viruses, because they can disable programs you want to use or use the minimally secure computer as a vector to infect other computer systems.

### **Standard Security**

Most often, computers are used to store sensitive and/or valuable data. This data could be anything from financial data to personnel files to personal correspondence. Also, you might need to protect against accidental or deliberate changes to the way the computer is set up. But the computer’s users need to be able to do their work, with minimal barriers to the resources they need.

### **Physical Security Considerations**

As with minimal security, the computer should be protected as any valuable equipment would be. Generally, this involves keeping the computer in a building that is locked to unauthorized users, as most homes and offices are. In some instances you might want to use a cable and lock to secure the computer to its location. If the computer has a physical lock, you can lock it and keep the key in a safe place for additional security. However, if the key is lost or inaccessible, an authorized user might be unable to work on the computer.

### **Standard Software Security Considerations**

A secure system requires effort from both the system administrators, who maintain certain software settings, and the everyday users, who must cultivate habits such as logging off at the end of the day and memorizing (rather than writing down) their passwords.

### Displaying a Legal Notice Before Log On

Windows NT can display a message box with the caption and text of your choice before a user logs on. Many organizations use this message box to display a warning message that notifies potential users that they can be held legally liable if they attempt to use the computer without having been properly authorized to do so. The absence of such a notice could be construed as an invitation, without restriction, to enter and browse the system.

The log on notice can also be used in settings (such as an information kiosk) where users might require instruction on how to supply a user name and password for the appropriate account.

To display a legal notice, use the Registry Editor to create or assign the following registry key values on the workstation to be protected:

Hive:	HKEY_LOCAL_MACHINE\SOFTWARE
Key:	\Microsoft\Windows NT\Current Version\Winlogon
Name:	LegalNoticeCaption
Type:	REG_SZ
Value:	Whatever you want for the title of the message box
Hive:	HKEY_LOCAL_MACHINE\SOFTWARE
Key:	Microsoft\Windows NT\Current Version\Winlogon
Name:	LegalNoticeText
Type:	REG_SZ
Value:	Whatever you want for the text of the message box

The changes take effect the next time the computer is started. You might want to update the Emergency Repair Disk to reflect these changes.

### Examples

Welcome to the XYZ Information Kiosk

Log on using account name Guest and password XYZCorp.

Authorized Users Only

Only individuals currently assigned an account on this computer by XYZCorp may access data on this computer. All information stored on this computer is the property of XYZCorp and is subject to all the protections accorded intellectual property.

## **User Accounts and Groups**

With standard security, a user account (user name) and password should be required in order to use the computer. You can establish, delete, or disable user accounts with User Manager, which is in the Administrative Tools program group. User Manager also allows you to set password policies and organize user accounts into Groups.

Note: Changes to the Windows NT computer user rights policy take effect when the user next logs on.

## **Administrative Accounts vs. User Accounts**

Use separate accounts for administrative activity and general user activity. Individuals who do administrative work on the computer should each have two user accounts on the system: one for administrative tasks, and one for general activity. To avoid accidental changes to protected resources; the account with the least privilege that can do the task at hand should be used. For example, viruses can do much more damage if activated from an account with administrator privileges.

It is a good idea to rename the built-in Administrator account to something less obvious. This powerful account is the one account that can never be locked out due to repeated failed log on attempts, and consequently is attractive to hackers who try to break in by repeatedly guessing passwords. By renaming the account, you force hackers to guess the account name as well as the password.

## **The Guest Account**

Limited access can be permitted for casual users through the built-in Guest account. If the computer is for public use, the Guest account can be used for public log ons. Prohibit Guest from writing or deleting any files, directories, or registry keys (with the possible exception of a directory where information can be left).

In a standard security configuration, a computer that allows Guest access can also be used by other users for files that they don't want accessible to the general public. These users can log on with their own user names and access files in directories on which they have set the appropriate permissions. They will want to be especially careful to log off or lock the workstation before they leave it. The Guest account is discussed in Chapter 2 "Working with User and Group Accounts" in *Microsoft Windows NT Server Concepts and Planning*. For procedural information, see Help.

## **Logging On**

All users should *always* press CTRL+ALT+DEL before logging on. Programs designed to collect account passwords can appear as a log on screen that is there waiting for you. By pressing CTRL+ALT+DEL you can foil these programs and get the secure log on screen provided by Windows NT.

## **Logging Off or Locking the Workstation**

Users should either log off or lock the workstation if they will be away from the computer for any length of time. Logging off allows other users to log on (if they know the password to an account); locking the workstation does not. The workstation can be set to lock automatically if it is not used for a set period of time by using any 32-bit screen saver with the Password Protected option. For information about setting up screen savers, see Help.

## **Passwords**

Anyone who knows a user name and the associated password can log on as that user. Users should take care to keep their passwords secret. Here are a few tips:

- Change passwords frequently, and avoid reusing passwords.
- Avoid using easily guessed words and words that appear in the dictionary. A phrase or a combination of letters and numbers works well.
- Don't write a password down—choose one that is easy for you to remember.

## **Protecting Files and Directories**

The NTFS file system provides more security features than the FAT system and should be used whenever security is a concern. The only reason to use FAT is for the boot partition of an ARC-compliant RISC system. A system partition using FAT can be secured in its entirety using the **Secure System Partition** command on the **Partition** menu of the Disk Administrator utility.

With NTFS, you can assign a variety of protections to files and directories, specifying which groups or individual accounts can access these resources in which ways. By using the inherited permissions feature and by assigning permissions to groups rather than to individual accounts, you can simplify the chore of maintaining appropriate protections. For more information, see Chapter 4, "Managing Shared Resources and Resource Security" in *Microsoft Windows NT Server Concepts and Planning*. For procedural information, see Help.

For example, a user might copy a sensitive document to a directory that is accessible to people who should not be allowed to read the document, thinking that the protections assigned to the document in its old location would still apply. In this case the protections should be set on the document as soon as it is copied, or else it should be first moved to the new directory, then copied back to the original directory.

On the other hand, if a file that was created in a protected directory is being placed in a shared directory so that other users can read it, it should be copied to the new directory; or if it is moved to the new directory, the protections on the file should be promptly changed so that other users can read the file.

When permissions are changed on a file or directory, the new permissions apply any time the file or directory is subsequently opened. Users who already have the file or directory open when you change the permissions are still allowed access according to the permissions that were in effect when they opened the file or directory.

## **Backups**

Regular backups protect your data from hardware failures and honest mistakes, as well as from viruses and other malicious mischief. The Windows NT Backup utility is described in Chapter 6, "Backing Up and Restoring Network Files" in *Microsoft Windows NT Server Concepts and Planning*. For procedural information, see Help.

Obviously, files must be read to be backed up, and they must be written to be restored. Backup privileges should be limited to administrators and backup operators—people to whom you are comfortable giving read and write access on all files.

### Protecting the Registry

All the initialization and configuration information used by Windows NT is stored in the registry. Normally, the keys in the registry are changed indirectly, through the administrative tools such as the Control Panel. This method is recommended. The registry can also be altered directly, with the Registry Editor; some keys can be altered in no other way.

The Registry Editor supports remote access to the Windows NT registry. To restrict network access to the registry, use the Registry Editor to create the following registry key:

Hive:	HKEY_LOCAL_MACHINE
Key:	\CurrentcontrolSet\Control\SecurePipeServers
Name:	\winreg

The security permissions set on this key define which users or groups can connect to the system for remote registry access. The default Windows NT Workstation installation does not define this key and does not restrict remote access to the registry. Windows NT Server permits only administrators remote access to the registry.

The Backup utility included with Windows NT allows you to back up the registry as well as files and directories.

**Note:** Registry Editor should be used only by individuals who thoroughly understand the tool, the registry itself, and the effects of changes to various keys in the registry. Mistakes made in the Registry Editor could render part or all of the system unusable.

### Auditing

Auditing can inform you of actions that could pose a security risk and also identify the user accounts from which audited actions were taken. Note that auditing only tells you what user accounts were used for the audited events. If passwords are adequately protected, this in turn indicates which user attempted the audited events. However, if a password has been stolen or if actions were taken while a user was logged on but away from the computer, the action could have been initiated by someone other than the person to whom the user account is assigned

When you establish an audit policy you'll need to weigh the cost (in disk space and CPU cycles) of the various auditing options against the advantages of these options. You'll want to at least audit failed log on attempts, attempts to access sensitive data, and changes to security settings. Here are some common security threats and the type of auditing that can help track them:

Threat	Action
Hacker-type break-in using random passwords	Enable failure auditing for log on and log off events.
Break-in using stolen password	Enable success auditing for log on and log off events. The log entries will not distinguish between the real users and the phony ones. What you are looking for here is unusual activity on user accounts, such as log ons at odd hours or on days when you would not expect any activity.
Misuse of administrative privileges by authorized users	Enable success auditing for use of user rights; for user and group management, for security policy changes; and for restart, shutdown, and system events. (Note: Because of the high volume of events that would be recorded, Windows NT does not normally audit the use of the Backup Files And Directories and the Restore Files And Directories rights. Appendix B, "Security In a Software Development Environment," explains how to enable auditing of the use of these rights.)
Virus outbreak	Enable success and failure write access auditing for program files such as files with .exe and .dll extensions. Enable success and failure process tracking auditing. Run suspect programs and examine the security log for unexpected attempts to modify program files or creation of unexpected processes. Note that these auditing settings generate a large number of event records during routine system use. You should use them only when you are actively monitoring the system log.
Improper access to sensitive files	Enable success and failure auditing for file- and object-access events, and then use File Manager to enable success and failure auditing of read and write access by suspect users or groups for sensitive files.
Improper access to printers	Enable success and failure auditing for file- and object-access events, and then use Print Manager to enable success and failure auditing of print access by suspect users or groups for the printers.

### High-Level Security

Standard security precautions are sufficient for most installations. However, additional precautions are available for computers that contain sensitive data, or that are at high risk for data theft or the accidental or malicious disruption of the system.

## Physical Security Considerations

The physical security considerations described for minimal and standard security configurations also apply here. In addition, you might want to examine the physical link provided by your computer network, and in some cases use controls built in to certain hardware platforms to restrict who can turn on the computer.

## Networks and Security

When you put a computer on a network, you add an access route to the computer, and you'll want that route to be secure. User validation and protections on files and other objects are sufficient for standard-level security, but for high-level security you'll need to make sure the network itself is secure, or in some cases isolate the computer completely.

The two risks from network connections are other network users and unauthorized network taps. If everyone on the network needs to access your secure computer, you will probably prefer to include the computer in the network to make it easier for these people to access data on the computer.

If the network is entirely contained in a secure building, the risk of unauthorized taps is minimized or eliminated. If the cabling must pass through unsecured areas, use optical fiber links rather than twisted pair to foil attempts to tap the wire and collect transmitted data.

If your installation needs access to the Internet, be aware of the security issues involved in providing access to—and from—the Internet community. Chapter 2, "Server Security on the Internet," in the *Windows NT Server Internet Guide* contains information on using network topology to provide security.

## Controlling Access to the Computer

No computer will ever be completely secure if people other than authorized users can physically access it. For maximum security on a computer that is not physically secure (locked safely away), follow all or some of the following security measures:

- Disable the floppy based boot if the computer hardware provides the option. If the computer doesn't require a floppy disk drive, remove it.
- The CPU should have a case that cannot be opened without a key. The key should be stored safely away from the computer.
- The entire hard disk should be NTFS.
- If the computer doesn't require network access, remove the network card.

## Controlling Access to the Power Switch

You might choose to keep unauthorized users away from the power or reset switches on the computer, particularly if your computer's rights policy denies them the right to shut down the computer. The most secure computers (other than those in locked and guarded rooms) expose only the computer's keyboard, monitor, mouse, and (when

appropriate) printer to users. The CPU and removable media drives can be locked away where only specifically authorized personnel can access them.

On many hardware platforms, the system can be protected using a *power-on password*. A power-on password prevents unauthorized personnel from starting an operating system other than Windows NT, which would compromise system security. Power-on passwords are a function of the computer hardware, not the operating system software. Therefore the procedure for setting up the power-on password depends on the type of computer and is available in the vendor's documentation supplied with the system.

## High-Level Software Security Considerations

Some high-security options can be implemented only by using the Registry Editor. The Registry Editor should be used only by administrators who are familiar with the material in Part V of *Windows NT Workstation Resource Guide*.

### User Rights

There are several user rights that administrators of high-security installations should be aware of and possibly audit. Of these, you might want to change the default permissions on three rights, as follows:

User Right	Groups assigned this right by default on workstation & stand-alone server	Recommended change for workstation & stand-alone server	Groups assigned this right by default on domain controller	Recommended change for domain controller
Log on locally. Allows a user to log on at the computer, from the computer's keyboard.	Administrators, Everyone, Guests, Power Users, and Users	Remove Everyone and Guests from having this right.	Account Operators, Administrators, Backup Operators, Server Operators, Print Operators	No Change
Shut down the system. (SeShutdown-Privilege) Allows a user to shut down Windows NT.	Administrators, Everyone, Guests, Power Users, and Users	Remove Everyone, Guests and Users from having this right.	Account Operators, Administrators, Backup Operators, Server Operators, Print Operators	No Change

Access this computer from the network Allows a user to connect over the network to the computer	Administrators, Everyone and Power Users	Administrators, Power Users and Users	Administrators, Everyone	Administrators, Backup Operators, Server Operators, Print Operators, Users and Guests if it is enabled
--	--	---------------------------------------	--------------------------	--

The rights in the following table generally require no changes to the default settings, even in the most highly secure installations. However, it is advisable to walk through the list and make any changes as per the needs of a particular installation.

<u>User Right</u>	<u>Groups assigned this right by default on workstation</u>	<u>Groups assigned this right by default on server</u>
Act as part of the operating system (SeTcbPrivilege) Allows a process to perform as a secure, trusted part of the operating system. Some subsystems are granted this right.	(None)	(None)
<u>User Right</u>	<u>Groups assigned this right by default on workstation</u>	<u>Groups assigned this right by default on server</u>
Add workstations to the domain (SeMachineAccountPrivilege) Allows users to added workstations to a particular domain. This right is meaningful only on domain controllers.	(None)	(None)
Back up files and directories (SeBackupPrivilege) Allows a user to back up files and directories. This right supersedes file and directory permissions.	Administrators, Backup Operators, Server Operators	Administrators, Backup Operators, Server Operators
Bypass traverse checking (SeChangeNotifyPrivilege) Allows a user to change directories and access files and subdirectories even if the user has no permission to access parent directories.	Everyone	Everyone

Change the system time (SeSystemTimePrivilege) Allows a user to set the time for the internal clock of the computer.	Administrators, Power Users	Administrators, Server Operators
Create a pagefile (SeCreatePagefilePrivilege) Allows the user to create new pagefiles for virtual memory swapping.	Administrators	Administrators
Create a token object (SeCreateTokenPrivilege) Allows a process to create access tokens. Only the Local Security Authority can do this.	(None)	(None)
Create permanent shared objects (SeCreatePermanentPrivilege) Allows user to create special permanent objects, such as \\Device, that are used within Windows NT.	(None)	(None)
Debug programs (SeDebugPrivilege) Allows a user to debug various low-level objects such as threads.	Administrators	Administrators
Force shutdown from a remote system (SeRemoteShutdownPrivilege) Allows the user to shutdown a Windows NT system remotely over a network.	Administrators, Power Users	Administrators, Server Operators
Generate security audits (SeAuditPrivilege) Allows a process to generate security audit log entries.	(None)	(None)
Increase quotas (SeIncreaseQuotaPrivilege) Nothing. This right has no effect in current versions of Windows NT.	Administrators	Administrators
<b>User Right</b>	<b>Groups assigned this right by default on workstation</b>	<b>Groups assigned this right by default on server</b>
Increase scheduling priority (SeIncreaseBasePriorityPrivilege) Allows a user to boost the execution priority of a process.	Administrators	Administrators
Load and unload device drivers (SeLoadDriverPrivilege) Allows a user to install and remove device drivers.	Administrators	Administrators

<p>Lock pages in memory (SeLockMemoryPrivilege)</p> <p>Allows a user to lock pages in memory so they cannot be paged out to a backing store such as Pagefile.sys.</p>	(None)	(None)
<p>Log on as a batch job</p> <p>Nothing. This right has no effect in current versions of Windows NT.</p>	(None)	(None)
<p>Log on as a service</p> <p>Allows a process to register with the system as a service.</p>	(None)	(None)
<p>Manage auditing and security log (SeSecurityPrivilege)</p> <p>Allows a user to specify what types of resource access (such as file access) are to be audited, and to view and clear the security log. Note that this right does not allow a user to set system auditing policy using the Audit command in the Policy menu of User Manager. Also, members of the administrators group always have the ability to view and clear the security log.</p>	Administrators	Administrators
<p>Modify firmware environment variables (SeSystemEnvironmentPrivilege)</p> <p>Allows a user to modify system environment variables stored in nonvolatile RAM on systems that support this type of configuration.</p>	Administrators	Administrators
<p>Profile single process (SeProfSingleProcess)</p> <p>Allows a user to perform profiling (performance sampling) on a process.</p>	Administrators	Administrators
<p>Profile system performance (SeSystemProfilePrivilege)</p> <p>Allows a user to perform profiling (performance sampling) on the system.</p>	Administrators	Administrators
<p>Replace a process-level token (SeAssignPrimaryTokenPrivilege)</p> <p>Allows a user to modify a process's security access token. This is a powerful right used only by the system.</p>	(None)	(None)
<b>User Right</b>	<b>Groups assigned this right by default on workstation</b>	<b>Groups assigned this right by default on server</b>
<p>Restore files and directories (SeRestorePrivilege)</p> <p>Allows a user to restore backed-up files and directories. This right supersedes file and directory permissions.</p>	Administrators, Backup Operators	Administrators, Server Operators, Backup Operators

Take ownership of files or other objects (SeTakeOwnershipPrivilege) Allows a user to take ownership of files, directories, printers, and other objects on the computer. This right supersedes permissions protecting objects.	Administrators	Administrators
--	----------------	----------------

## Protecting Files and Directories

Among the files and directories to be protected are those that make up the operating system software itself. The standard set of permissions on system files and directories provide a reasonable degree of security without interfering with the computer's usability. For high-level security installations, however, you might want to additionally set directory permissions to all subdirectories and existing files, as shown in the following list, *immediately after Windows NT is installed*. Be sure to apply permissions to parent directories before applying permissions to subdirectories.

First apply the following using the ACL editor:

Directory	Permissions
\WINNT and <i>all subdirectories</i> under it.	Administrators: Full Control CREATOR OWNER: Full Control Everyone: Read SYSTEM: Full Control

Now, within the \WINNT tree, apply the following exceptions to the general security:

Directory	Permissions
\WINNT\REPAIR	Administrators: Full Control
\WINNT\SYSTEM32\CONFIG	Administrators: Full Control CREATOR OWNER: Full Control Everyone: List SYSTEM: Full Control
\WINNT\SYSTEM32\SPOOL	Administrators: Full Control CREATOR OWNER: Full Control Everyone: Read Power Users: Change SYSTEM: Full Control

\WINNT\COOKIES \WINNT\FORMS \WINNT\HISTORY \WINNT\OCCACHE \WINNT\PROFILES \WINNT\SENDTO \WINNT\Temporary Internet Files	Administrators: Full Control CREATOR OWNER: Full Control Everyone: Special Directory Access – Read, Write and Execute, Special File Access – None System : Full Control
---	--

Several critical operating system files exist in the root directory of the system partition on Intel 80486 and Pentium-based systems. In high-security installations you might want to assign the following permissions to these files:

File	C2-Level Permissions
\Boot.ini, \Ntdetect.com, \Ntldr	Administrators: Full Control SYSTEM: Full Control
\Autoexec.bat, \Config.sys	Everybody: Read Administrators: Full Control SYSTEM: Full Control
\TEMP directory	Administrators: Full Control SYSTEM: Full Control CREATOR OWNER: Full Control Everyone: Special Directory Access – Read, Write and Execute, Special File Access – None

To view these files in File Manager, choose the **By File Type** command from the **View** menu, then select the **Show Hidden/System Files** check box in the **By File Type** dialog box.

Note that the protections mentioned here are over and above those mentioned earlier in the standard security level section, which included having only NTFS partitions (except the boot partition in case of RISC machines). The FAT boot partition for RISC systems can be configured using the **Secure System Partition** command on the **Partition** menu of the Disk Administrator utility.

It is also highly advisable that Administrators manually scan the permissions on various partitions on the system and ensures that they are appropriately secured for various user accesses in their environment.

## Protecting the Registry

In addition to the considerations for standard security, the administrator of a high-security installation might want to set protections on certain keys in the registry.

By default, protections are set on the various components of the registry that allow work to be done while providing standard-level security. For high-level security, you might want to assign access rights to specific registry keys. This should be done with caution, because programs that the users require to do their jobs often need to access certain keys on the users' behalf. For more information, see Chapter 24, "Registry Editor and Registry Administration."

For each of the keys listed below, make the following change:

Access allowed	
Everyone Group	QueryValue, Enumerate Subkeys, Notify and Read Control

**In the HKEY\_LOCAL\_MACHINE on Local Machine dialog:**

\Software

This change is recommended. It locks the system in terms of who can install software. Note that it is **not** recommended that the entire subtree be locked using this setting because that can render certain software unusable.

\Software\Microsoft\RPC (and its subkeys)

This locks the RPC services.

\Software\Microsoft\Windows NT\ CurrentVersion

\Software\Microsoft\Windows NT\ CurrentVersion\Profile List

\Software\Microsoft\Windows NT\ CurrentVersion\AeDebug

\Software\Microsoft\Windows NT\ CurrentVersion\Compatibility

\Software\Microsoft\Windows NT\ CurrentVersion\Drivers

\Software\Microsoft\Windows NT\ CurrentVersion\Embedding

\Software\Microsoft\Windows NT\ CurrentVersion\Fonts

\Software\Microsoft\Windows NT\ CurrentVersion\FontSubstitutes

\Software\Microsoft\Windows NT\ CurrentVersion\Font Drivers

\Software\Microsoft\Windows NT\ CurrentVersion\Font Mapper

\Software\Microsoft\Windows NT\ CurrentVersion\Font Cache

\Software\Microsoft\Windows NT\ CurrentVersion\GRE\_Initialize

\Software\Microsoft\Windows NT\ CurrentVersion\MCI

\Software\Microsoft\Windows NT\ CurrentVersion\MCI Extensions

\Software\Microsoft\Windows NT\ CurrentVersion\PerfLib

Consider removing Everyone:Read access on this key. This allows remote users to see performance data on the machine. Instead you could give INTERACTIVE:Read Access which will allow only interactively logged on user access to this key, besides administrators and system.

\Software\Microsoft\Windows NT\ CurrentVersion\Port (and all subkeys)

\Software\Microsoft\Windows NT\ CurrentVersion\Type1 Installer

\Software\Microsoft\Windows NT\ CurrentVersion\WOW (and all subkeys)

\Software\Microsoft\Windows NT\ CurrentVersion\Windows3.1MigrationStatus (and all subkeys)

\System\CurrentControlSet\Services\LanmanServer\Shares

\System\CurrentControlSet\Services\UPS

Note that besides setting security on this key, it is also required that the command file (if any) associated with the UPS service is appropriately secured, allowing Administrators: Full Control, System: Full Control only.

\Software\Microsoft\Windows\CurrentVersion\Run

\Software\Microsoft\Windows\CurrentVersion\RunOnce

\Software\Microsoft\Windows\CurrentVersion\Uninstall

**In the HKEY\_CLASSES\_ROOT on Local Machine dialog:**

HKEY\_CLASSES\_ROOT (and all subkeys)

**In the HKEY\_USERS on Local Machine dialog:**

\.DEFAULT

The Registry Editor supports remote access to the Windows NT registry. To restrict network access to the registry, use the Registry Editor to create the following registry key:

Hive:	HKEY_LOCAL_MACHINE
Key:	System\CurrentcontrolSet\Control\SecurePipeServers
Name:	\winreg

The security permissions set on this key define which users or groups can connect to the system for remote registry access. The default Windows NT Workstation installation does not define this key and does not restrict remote access to the registry. Windows NT Server permits only administrators remote access to most of the registry. Some paths that need to be accessible by non-administrators are specified in the HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\SecurePipeServers\winreg\AllowedPaths key.

In the environments where members of server operators are not sufficiently trusted, it is recommended that security on following keys be changed as below:

Registry Key	Recommended Permissions
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon	CREATOR OWNER: Full Control Administrators: Full Control SYSTEM: Full Control Everyone: Read

### Secure EventLog Viewing

Default configuration allows guests and null log ons ability to view event logs (system, and application logs). Security log is protected from guest access by default, it is viewable by users who have "Manage Audit Logs" user right. The Event log services use the following key to restrict guest access to these logs:

Hive:	HKEY_LOCAL_MACHINE
Key:	\System\CurrentControlSet\Services\EventLog\[LogName]
Name:	RestrictGuestAccess
Type	REG_DWORD
Value:	1

Set the value for each of the logs to 1. The change takes effect on next reboot. Needless to say that you will have to change the security on this key to disallow everyone other than Administrators and System any access because otherwise malicious users can reset these values.

### Secure Print Driver Installation

Registry key AddPrinterDrivers under HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers, Key value AddPrinterDrivers (REG\_DWORD) is used to control

who can add printer drivers using the print folder. This key value should be set to 1 to enable the system spooler to restrict this operation to administrators and print operators (on server) or power users (on workstation).

Hive:	HKEY_LOCAL_MACHINE
Key:	System\CurrentcontrolSet\Control\Print\Providers\LanMan Print Services\Servers
Name:	AddPrintDrivers
Type	REG_DWORD
Value:	1

### The Schedule Service (AT Command)

The Schedule service (also known as the **AT** command) is used to schedule tasks to run automatically at a preset time. Because the scheduled task is run in the context run by the Schedule service (typically the operating system's context), this service should not be used in a highly secure environment.

By default, only administrators can submit **AT** commands. To allow system operators to also submit **AT** commands, use the Registry Editor to create or assign the following registry key value:

Hive:	HKEY_LOCAL_MACHINE\SYSTEM
Key:	\CurrentControlSet\Control\Lsa
Name:	Submit Control
Type:	REG_DWORD
Value:	1

There is no way to allow anyone else to submit **AT** commands. Protecting the registry as explained earlier restricts direct modification of the registry key using the registry editor. Access to the registry key

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\ Services\Schedule should also be restricted to only those users/groups (preferably Administrators only) that are allowed to submit jobs to the schedule service.

Registry Key	Recommended Permissions
HKEY_LOCAL_MACHINE\System\CurrentControlSet\ Services\Schedule	CREATOR OWNER: Full Control Administrators: Full Control SYSTEM: Full Control Everyone: Read

The changes will take effect the next time the computer is started. You might want to update the Emergency Repair Disk to reflect these changes.

## Secure File Sharing

The native Windows NT file sharing service is provided using the SMB-based server and redirector services. Even though only administrators can create shares, the default security placed on the share allows Everyone full control access. These permissions are controlling access to files on down level file systems like FAT which do not have security mechanisms built in. Shares on NTFS enforce the security on the underlying directory it maps to and it is recommended that proper security be put via NTFS and not via the file sharing service.

Also note that the share information resides in the registry which also needs to be protected as explained in a section earlier.

Service Pack 3 for Windows NT version 4.0 includes several enhancements to SMB based file sharing protocol. These are: It supports mutual authentication to counter man-in-the-middle attacks.

- It supports message authentication to prevent active message attacks.

These are provided by incorporating message signing into SMB packets which are verified by both server and client ends. There are registry key settings to enable SMB signatures on each side.

To ensure that SMB server responds to clients with message signing only, configure the following two key values:

Hive:	HKEY_LOCAL_MACHINE\SYSTEM
Key:	System\CurrentControlSet\Services\LanManServer\Parameters
Name:	RequireSecuritySignature
Type:	REG_DWORD
Value:	1

Hive:	HKEY_LOCAL_MACHINE\SYSTEM
Key:	System\CurrentControlSet\Services\LanManServer\Parameters
Name:	EnableSecuritySignature
Type:	REG_DWORD
Value:	1

Setting these values ensures that the Server communicates with only those clients that are aware of message signing. Note that this means that installations that have multiple versions of client software, older versions will fail to connect to servers that have this key value configured. Also note that it is extremely important that both keys

be changed – setting RequireSecuritySignature without setting EnableSecuritySignature will prevent all access to the machine's SMB shares.

Similarly, security conscious clients can also decide to communicate with servers that support message signing and no one else.

Hive:	HKEY_LOCAL_MACHINE\SYSTEM
Key:	System\CurrentControlSet\Services\Rdr\Parameters
Name:	RequireSecuritySignature
Type:	REG_DWORD
Value:	1

Note that setting this key value implies that the client will not be able to connect to servers which do not have message signing support.

Please refer to Knowledge Base article Q161372 for further details on SMB message signing enhancements.

Windows NT version 4.0 Service Pack 3 also includes another enhancement to SMB file sharing protocol such that by default you are unable to connect to SMB servers (such as Samba or Hewlett-Packard (HP) LM/X or LAN Manager for UNIX) with an unencrypted (plain text) password. This protects from sending clear text forms of passwords over the wire. Please refer to Knowledge base article Q166730 if you have any reasons to allow clients to send unencrypted passwords over the wire.

Additionally, customers may want to delete the administrative shares (\$ shares) if they are not needed on an installation. This can be accomplished using "net share" command. For example:

```
C:\> net share admin$ /d
```

## FTP Service

Windows NT also comes with another standard Internet service called file transfer protocol (FTP). A common use of FTP is to allow public file access via *anonymous* log on. When configuring FTP server, the administrator assigns the server a user account for anonymous log ons and a default home directory. The default anonymous user account for FTP is GUEST. This should be changed to a different user account and should have a password. Also, this account should not be member of any privileged groups so that the only default group that shows up in the security token during log on is Everyone. The account should not be allowed "Logon on Locally" user right to restrict "insider attacks".

The home directory parameter should be configured carefully. FTP server exports entire disk partitions. The administrator can only configure which partitions are accessible via FTP but not which directories on that partition. Therefore, a user coming via FTP can move to directories "above" the home directory. Therefore, in general it is recommended that if FTP service needs to run on a system, it is best to assign a complete disk partition as the FTP store, and to make only that partition accessible via FTP.

## NetBios Access From Internet

For Windows NT systems with direct Internet connectivity and have NetBios, there are two configuration options:

- Configure the NT system on the Internet outside the corporate firewall. You can also accomplish this by blocking ports 135, 137 and 138 on TCP and UDP protocols at the firewall. This ensures that no NetBIOS traffic moves across the corporate firewall.
- Configure the protocol bindings between TCP/IP, NetBIOS, Server and Workstation services using the network control panel. By removing the bindings between NetBios and TCP/IP, the native file sharing services (using the Server and Workstation services) will not be accessible via TCP/IP and hence the Internet. These and other NetBios services will still be accessible via a local LAN-specific, non-routable protocol (ex: NetBEUI) if one is in place. To accomplish this use the Network Control Panel applet. Select the Bindings Tab and disable the NetBios bindings with TCP/IP protocol stack.

A Windows NT system with direct Internet connectivity needs to be secured with respect to other services besides NetBios access, specifically Internet Information Server. Please refer to Microsoft Internet Information Server: Security Overview white paper for details on this area.

## Hiding the Last User Name

By default, Windows NT places the user name of the last user to log on the computer in the User name text box of the **Logon** dialog box. This makes it more convenient for the most frequent user to log on. To help keep user names secret, you can prevent Windows NT from displaying the user name from the last log on. This is especially important if a computer that is generally accessible is being used for the (renamed) built-in Administrator account.

To prevent display of a user name in the Logon dialog box, use the Registry Editor to create or assign the following registry key value:

Hive:	HKEY_LOCAL_MACHINE\SOFTWARE
Key:	\Microsoft\Windows NT\Current Version\Winlogon
Name:	DontDisplayLastUserName
Type:	REG_SZ
Value:	1

## Restricting the Boot Process

Most personal computers today can start a number of different operating systems. For example, even if you normally start Windows NT from the C: drive, someone could select another version of Windows on another drive, including a floppy drive or CD-ROM drive. If this happens, security precautions you have taken within your normal version of Windows NT might be circumvented.

In general, you should install only those operating systems that you want to be used on the computer you are setting up. For a highly secure system, this will probably mean installing one version of Windows NT. However, you must still protect the CPU physically to ensure that no other operating system is loaded. Depending on your circumstances, you might choose to remove the floppy drive or drives. In some computers you can disable booting from the floppy drive by setting switches or jumpers inside the CPU. If you use hardware settings to disable booting from the floppy drive, you might want to lock the computer case (if possible) or lock the machine in a cabinet with a hole in the front to provide access to the floppy drive. If the CPU is in a locked area away from the keyboard and monitor, drives cannot be added or hardware settings changed for the purpose of starting from another operating system. Another simple setting is to edit the boot.ini file such that the boot timeout is 0 seconds; this will make hard for the user to boot to another system if one exists.

Other hardware configurations such as firmware setup, boot password, power-on password are also available on latest hardware to control the boot process and should be appropriately investigated and used.

### **Allowing Only Logged-On Users to Shut Down the Computer**

Normally, you can shut down a computer running Windows NT Workstation without logging on by choosing Shutdown in the **Logon** dialog box. This is appropriate where users can access the computer's operational switches; otherwise, they might tend to turn off the computer's power or reset it without properly shutting down Windows NT Workstation. However, you can remove this feature if the CPU is locked away. (This step is not required for Windows NT Server, because it is configured this way by default.)

To require users to log on before shutting down the computer, use the Registry Editor to create or assign the following Registry key value:

Hive:	HKEY_LOCAL_MACHINE\SOFTWARE
Key:	\Microsoft\Windows NT\Current Version\Winlogon
Name:	ShutdownWithoutLogon
Type:	REG_SZ
Value:	0

The changes will take effect the next time the computer is started. You might want to update the Emergency Repair Disk to reflect these changes.

## Controlling Access to Removable Media

By default, Windows NT allows any program to access files on floppy disks and CDs. In a highly secure, multi-user environment, you might want to allow only the person interactively logged on to access those devices. This allows the interactive user to write sensitive information to these drives, confident that no other user or program can see or modify that data.

When operating in this mode, the floppy disks and/or CDs on your system are allocated to a user as part of the interactive log on process. These devices are automatically freed for general use or for reallocation when that user logs off. Because of this, it is important to remove sensitive data from the floppy or CD-ROM drives before logging off.

Note: Windows NT allows all users access to the tape drive, and therefore any user can read and write the contents of any tape in the drive. In general this is not a concern, because only one user is interactively logged on at a time. However, in some rare instances, a program started by a user can continue running after the user logs off. When another user logs on and puts a tape in the tape drive, this program can secretly transfer sensitive data from the tape. If this is a concern, restart the computer before using the tape drive.

### To Allocate Floppy Drives During Log On

Use the Registry Editor to create or assign the following registry key value:

Hive:	HKEY_LOCAL_MACHINE\SOFTWARE
Key:	\Microsoft\WindowsNT\CurrentVersion\Winlogon
Name:	AllocateFloppies
Type:	REG_SZ
Value:	1

If the value does not exist, or is set to any other value, then floppy devices will be available for shared use by all processes on the system.

This value will take effect at the next log on. If a user is already logged on when this value is set, it will have no effect for that log on session. The user must log off and log on again to cause the device(s) to be allocated.

### To Allocate CD-ROMs During Log On

Use the Registry Editor to create or assign the following registry key value:

Hive:	HKEY_LOCAL_MACHINE\SOFTWARE
Key:	\Microsoft\WindowsNT\CurrentVersion\Winlogon

Name:	AllocateCDRoms
Type:	REG_SZ
Value:	1

If the value does not exist, or is set to any other value, then CD-ROM devices will be available for shared use by all processes on the system.

This value will take effect at the next log on. If a user is already logged on when this value is set, it will have no effect for that log on session. The user must log off and log on again to cause the device(s) to be allocated.

### **Securing Base System Objects**

To enable stronger protection on base objects, add the following value to the registry key HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\SessionManager:

Name: ProtectionMode  
Type: REG\_DWORD  
Value: 1

This registry setting informs the Windows NT Session Manager that security on the base system objects should be at C2 security level. Please refer to Appendix D of the Windows NT Resource Kit, Version 4.0 *Update Guide* for the impact of this setting.

### **Enabling System Auditing**

Enabling system auditing can inform you of actions that pose security risks and possibly detect security breaches.

To activate security event logging, follow these steps:

1. Log on as the administrator of the local workstation.
2. Click the Start button, point to Programs, point to Administrative Tools, and then click User Manager.
3. On the Policies menu, click Audit.
4. Click the Audit These Events option.
5. Enable the options you want to use. The following options are available:
  - Log on/Log off: Logs both local and remote resource logins.
  - File and Object Access: File, directory, and printer access.

- Note: Files and folders must reside on an NTFS partition for security logging to be enabled. Once the auditing of file and object access has been enabled, use Windows NT Explorer to select auditing for individual files and folders.
  - User and Group Management: Any user accounts or groups created, changed, or deleted. Any user accounts that are renamed, disabled, or enabled. Any passwords set or changed.
  - Security Policy Changes: Any changes to user rights or audit policies.
  - Restart, Shutdown, And System: Logs shutdowns and restarts for the local workstation.
  - Process Tracking: Tracks program activation, handle duplication, indirect object access, and process exit.
6. Click the Success check box to enable logging for successful operations, and the Failure check box to enable logging for unsuccessful operations.
  7. Click OK.

Note that Auditing is a “detection” capability rather than “prevention” capability. It will help you discover security breaches after they occur and therefore should always be considered in addition to various preventive measures.

### **Auditing Base Objects**

To enable auditing on base system objects, add the following key value to the registry key HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\Lsa:

Name: AuditBaseObjects

Type: REG\_DWORD

Value: 1

Note that simply setting this key does not start generating audits. The administrator will need to turn auditing on for the “Object Access” category using User Manager. This registry key setting tells Local Security Authority that base objects should be created with a default system audit control list.

### **Auditing of Privileges**

Certain privileges in the system are not audited by default even when auditing on privilege use is turned on. This is done to control the growth of audit logs. The privileges are:

1. Bypass traverse checking (given to everyone).
2. Debug programs (given only to administrators)
3. Create a token object (given to no one)
4. Replace process level token (given to no one)
5. Generate Security Audits (given to no one)

6. Backup files and directories (given to administrators and backup operators)
7. Restore files and directories (given to administrators and backup operators)

1 is granted to everyone so is meaningless from auditing perspective. 2 is not used in a working system and can be removed from administrators group. 3, 4 and 5 are not granted to any user or group and are highly sensitive privileges and should not be granted to anyone. However 6 and 7 are used during normal system operations and are expected to be used. To enable auditing of these privileges, add the following key value to the registry key HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\Lsa:

Name: FullPrivilegeAuditing  
Type: REG\_BINARY  
Value: 1

Note that these privileges are not audited by default because backup and restore is a frequent operation and this privilege is checked for every file and directory backed or restored, which can lead to thousands of audits filling up the audit log in no time. Carefully consider turning on auditing on these privilege uses.

### **Shutdown option on Full Audit Log**

In a C2 configured system, auditing system of Windows NT provides an option to the administrator to shut down the system when security audit log is filled up. To enable this, use the following key value in the registry key:

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\Lsa:

Name: CrashOnAuditFail  
Type: REG\_DWORD  
Value: 1

With this setting, the system will shutdown itself when the audit log full is detected. The value in the registry is reset to 2. When the system is rebooted, it only allows the administrators to log on to the machine (locally or remotely). They will be required to clean the audit log (or archive it), reset the value to 1 and reboot the system before any other user is allowed to log on.

### **Enhanced Protection for Security Accounts Manager Database**

The Windows NT Server 4.0 System Key hotfix (included in Service Pack 3) provides the capability to use strong encryption techniques to increase protection of account password information stored in the registry by the Security Account Manager (SAM). Windows NT Server stores user account information, including a derivative of the user account password, in a secure portion of the Registry protected by access control and an obfuscation function. The account information in the Registry is only accessible to members of the Administrators group. Windows NT Server, like other operating systems, allows privileged users who are administrators access to all resources in the

system. For installations that want enhanced security, strong encryption of account password derivative information provides an additional level of security to prevent Administrators from intentionally or unintentionally accessing password derivatives using Registry programming interfaces.

Please refer to Knowledge Base article Q143475 for more details on SysKey feature and how it can be implemented on a Windows NT installation.

### **Restricting Anonymous network access to Registry**

Windows NT version 4.0 Service Pack 3 includes a security enhancement that restricts anonymous (null session) logons when they connect to specific named pipes including the one for Registry.

There is a registry key value that defines the list of named pipes that are "exempt" from this restriction. The key value is:

Hive:	HKEY_LOCAL_MACHINE\SYSTEM
Key:	System\CurrentControlSet\Services\LanManServer\Parameters
Name:	NullSessionPipes
Type:	REG_MULTI_SZ
Value:	Add or Remove names from the list as required by the configuration.

Please refer to Knowledge Base article Q143138 for more details.

### **Restricting Anonymous network access to lookup account names and groups and network shares**

Windows NT has a feature where anonymous logon users can list domain user names and enumerate share names. Customers who want enhanced security have requested the ability to optionally restrict this functionality. Windows NT 4.0 Service Pack 3 and a hotfix for Windows NT 3.51 provide a mechanism for administrators to restrict the ability for anonymous logon users (also known as NULL session connections) to list account names and enumerate share names. Listing account names from Domain Controllers is required by the Windows NT ACL editor, for example, to obtain the list of users and groups to select who a user wants to grant access rights. Listing account names is also used by Windows NT Explorer to select from list of users and groups to grant access to a share.

The registry key value to set for enabling this feature is:

Hive:	HKEY_LOCAL_MACHINE\SYSTEM
Key:	System\CurrentControlSet\Control\LSA
Name:	RestrictAnonymous
Type:	REG_DWORD

Value:	1.
--------	----

This enhancement is part of Windows NT version 4.0 Service Pack 3. A hot fix for it is also provided for Windows NT version 3.51. Please refer to Knowledge Base article Q143474 for more details on this.

### Enforcing strong user passwords

Windows NT 4.0 Service Pack 2 and later includes a password filter DLL file (Passfilt.dll) that lets you enforce stronger password requirements for users. Passfilt.dll provides enhanced security against "password guessing" or "dictionary attacks" by outside intruders.

Passfilt.dll implements the following password policy:

- Passwords must be at least six (6) characters long. (The minimum password length can be increased further by setting a higher value in the Password Policy for the domain).
- Passwords must contain characters from at least three (3) of the following four (4) classes:

Description	Examples
English upper case letters	A, B, C, ... Z
English lower case letters	a, b, c, ... z
Westernized Arabic numerals	0, 1, 2, ... 9
Non-alphanumeric ("special characters") such as punctuation symbols	

- Passwords may not contain your user name or any part of your full name.

These requirements are hard-coded in the Passfilt.dll file and cannot be changed through the user interface or registry. If you wish to raise or lower these requirements, you may write your own .dll and implement it in the same fashion as the Microsoft version that is available with Windows NT 4.0 Service Pack 2.

To use Passfilt.Dll, the administrator must configure the password filter DLL in the system registry on all domain controllers. This can be done as follows:

- Setup the following registry key value:

Hive:	HKEY_LOCAL_MACHINE\SYSTEM
Key:	System\CurrentControlSet\Control\LSA
Name:	Notification Packages
Type:	REG_MULTI_SZ
Value:	Add string "PASSFILT" (do not remove existing ones).

**Disabling LanManager Password Hash Support** Windows NT supports the following two types of challenge/response authentication:

- LanManager (LM) challenge/response
- Windows NT challenge/response

To allow access to servers that only support LM authentication, Windows NT clients currently send both authentication types. Microsoft developed a patch that allows clients to be configured to send only Windows NT authentication. This removes the use of LM challenge/response messages from the network.

Applying this hot fix, configures the following registry key:

Hive:	HKEY_LOCAL_MACHINE\SYSTEM
Key:	System\CurrentControlSet\Control\LSA
Name:	LMCompatibilityLevel
Type:	REG_DWORD
Value:	0,1,2 (Default 0)

Setting the value to:

- 0 – Send both Windows NT and LM password forms.
- 1 – Send Windows NT and LM password forms only if the server requests it.
- 2 – Never send LM password form.

If a Windows NT client selects level 2, it cannot connect to servers that support only LM authentication, such as Windows 95 and Windows for Workgroups.

For more complete information on this hot fix, please refer to Knowledge Base article number Q147706.

### **Wiping the System Page File during clean system shutdown**

Virtual Memory support of Windows NT uses a system page file to swap pages from memory of different processes onto disk when they are not being actively used. On a running system, this page file is opened exclusively by the operating system and hence is well-protected. However, systems that are configured to allow booting to other operating systems, may want to ensure that system page file is wiped clean when Windows NT shuts down. This ensures that sensitive information from process memory that may have made into the page file is not available to a snooping user. This can be achieved by setting up the following key:

Hive:	HKEY_LOCAL_MACHINE\SYSTEM
-------	---------------------------

Key:	System\CurrentControlSet\Control\SessionManager\Memory Management
Name:	ClearPageFileAtShutdown
Type:	REG_DWORD
Value:	1

Note that, this protection works only during a clean shutdown, therefore it is important that untrusted users do not have ability to power off or reset the system manually.

### **Disable Caching of Logon Credentials during interactive logon.**

The default configuration of Windows NT caches the last logon credentials for a user who logged on interactively to a system. This feature is provided for system availability reasons such as the user's machine is disconnected or none of the domain controllers are online.

Even though the credential cache is well protected, in a highly secure environments, customers may want to disable this feature. This can be done by setting the following registry key:

Hive:	HKEY_LOCAL_MACHINE
Key:	Software\Microsoft\Windows NT\CurrentVersion\Winlogon
Name:	CachedLogonsCount
Type:	REG_SZ
Value:	0

## **C2 Security**

The National Computer Security Center (NCSC) is the United States government agency responsible for performing software product security evaluations. These evaluations are carried out against a set of requirements outlined in the NCSC publication *Department of Defense Trusted Computer System Evaluation Criteria*, which is commonly referred to as the "Orange Book."

Windows NT has been successfully evaluated by the NCSC at the C2 security level as defined in the Orange Book, which covers the base operating system.

In addition, Windows NT is currently under evaluation for its networking component of a secure system in compliance to the NCSC's "Red Book." The Red Book is an interpretation of the Orange Book as applies to network security.

Some of the most important requirements of C2-level security are the following:

- The owner of a resource (such as a file) must be able to control access to the resource.
- The operating system must protect objects so that other processes do not randomly reuse them. For example, the system protects memory so that its contents cannot be read after a process frees it. In addition, when a file is deleted, users must not be able to access the data from that file.
- Each user must identify him or her by typing a unique log on name and password before being allowed access to the system. The system must be able to use this unique identification to track the activities of the user.
- System administrators must be able to audit security-related events. Access to this audit data must be limited to authorized administrators.
- The system must protect itself from external interference or tampering, such as modification of the running system or of system files stored on disk.

### **Evaluation vs. Certification**

The NCSC evaluation process does a good job of ensuring that Windows NT can properly enforce your security policy, but it does not dictate what your security policy must be. There are many features of Windows NT that need to be considered when determining how to use the computer within your specific environment. What level of auditing will you require? How should your files be protected to ensure that only the right people could access them? What applications should you allow people to run? Should you use a network? If so, what level of physical isolation of the actual network cable is needed?

To address the environmental aspects of a computing environment, the NCSC has produced a document called *Introduction to Certification and Accreditation*. In this document, “certification” is described as a plan to use computer systems in a specific environment, and “accreditation” is the evaluation of that plan by administrative authorities. It is this certification plan, and the subsequent accreditation procedure, that balances the sensitivity of the data being protected against the environmental risks present in the way the computing systems are used. For example, a certification plan for a university computing lab might require that computers be configured to prevent starting from a floppy disk, to minimize the risk of infection by virus or Trojan Horse programs. In a top-secret Defense Department development lab, it might be necessary to have a fiber-optic LAN to prevent generation of electronic emissions. A good certification plan covers all aspects of security, from backup/recovery mechanisms to the Marine guards standing at the front door of your building.

### **Additional C2 Evaluation Information**

If you need to set up a C2-certifiable system, see Chapter 2, “Microsoft Report on C2 Evaluation of Windows NT.” That chapter lists the hardware configurations in which Windows NT has been evaluated. Chapter 2 also specifies the set of features that were implemented for C2 evaluation so that you can duplicate them if necessary for your own C2-certifiable system. These features are essentially those recommended for high-level security in this chapter.

For your C2 certification, you will need to choose the combination of security features described in this chapter, in Chapter 2 of *Windows NT Server Networking Guide*, and in the Windows NT documentation that fits your particular combination of resources, personnel, work flow, and perceived risks. You might also want to study Appendix B, "Security in a Software Development Environment," especially if you are using custom or in-house software. This appendix also provides information on managing and interpreting the security log and technical details on special-case auditing (for example, auditing base objects).

### **Setting up a C2-compliant System**

To make it easier to set up a C2-compliant system, the C2Config application has been created and included in the Windows NT 4.0 Resource Kit. C2config.exe lets you choose from the settings used in evaluating Windows NT for C2 security, and implement the settings you want to use in your installation. For details, see the online Help included with the application.