
Guide to Securing Microsoft Windows 2000[®] File and Disk Resources

**Field Security Operations of the
Defense Information Systems Agency (DISA)
and the
System and Network Attack Center of the
National Security Agency**

Authors:
Owen R. McGovern, EDS,
DISA
Julie M. Haney, NSA



Updated: November 26, 2002
Version 1.0.1

**DISA FSO
D3314, Bldg 1
1 Overcash Avenue, LEAD
Chambersburg, PA 17201-4122**

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

W2KGuides@nsa.gov

Change Control

Version	Date	Details
1.0.1	26 Nov. 2002	Added this change control section to track version modifications. Page 19, added a note under the "Deleting subsystem registry key values" section.

Warnings

- **Do not attempt to implement any of the settings in this guide without first testing in a non-operational environment.**
- This document is only a guide containing recommended security settings. It is not meant to replace well-structured policy or sound judgment. Furthermore this guide does not address site-specific configuration issues. Care must be taken when implementing this guide to address local operational and policy concerns.
- The security changes described in this document only apply to Microsoft Windows 2000 systems and should not be applied to any other Windows versions or operating systems.
- SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE EXPRESSLY DISCLAIMED. IN NO EVENT SHALL THE CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
- This document is current as of April 19, 2001. See Microsoft's web page <http://www.microsoft.com/> for the latest changes or modifications to the Windows 2000 operating system.

UNCLASSIFIED

This Page Intentionally Left Blank

UNCLASSIFIED

Acknowledgements

The authors would like to acknowledge the authors of the “*Guide to Implementing Windows NT in Secure Network Environments*” and the “*Guide to Securing Microsoft Windows NT Networks*” versions 2.0, 2.1, 3.0, 4.0, and 4.1. Significant portions of this document were taken from the NSA “*Guide to Securing Microsoft Windows NT Networks*” by Paul Bartock, et. al., and the “*Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Toolset*” by Julie Haney.

The authors would like to acknowledge Ms. Terry M. Powell, EDS, Paul Bartock, NSA, the NSA Windows 2000 team for their review and recommendations, and Ms. Robin Langlois, DISA FSO, for coordinating communications between the collaborating parties.

Some parts of this document were drawn from Microsoft copyright materials with their permission.

Trademark Information

Microsoft, MS-DOS, Windows, Windows 2000, Windows NT, Windows 98, Windows 95, Windows for Workgroups, and Windows 3.1 are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and other countries.

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

Table of Contents

Warnings	iii
<i>Acknowledgements</i>	v
Trademark Information	vi
Table of Contents	vii
Table of Figures	ix
Table of Tables	x
Introduction	1
<i>Getting the Most from this Guide</i>	1
<i>About the Guide to Securing Microsoft Windows 2000 File and Disk Resources</i>	1
Chapter 1 Securing the Windows 2000 File System	3
<i>NTFS</i>	3
Converting to NTFS	3
Default Security Templates	4
<i>File and Folder Permissions</i>	4
<i>Securing File and Folder Access Control Lists</i>	7
<i>Additional File System Security Measures</i>	8
Removing the OS/2 and Posix subsystems	8
Deleting subsystem executables	8
Deleting subsystem registry key values	9
Removing Leftover Directories on Upgraded Systems	9
Preventing Data Remanence	10
Recycle Bin	10
System Page File	10
Chapter 2 Shared Resources	11
<i>Setting Share Permissions</i>	11
<i>Share Security Recommendations</i>	11
<i>Restricting anonymous listing of shares</i>	12
Chapter 3 File Auditing	13
<i>Auditing Policy</i>	13
<i>File Auditing</i>	14
Adding Audit Settings on a File or Folder	15
Modifying Audit Settings on a File or Folder	16
Chapter 4 Securing Disk Resources	17
<i>Physical Security</i>	17
<i>Securing Disk Resources at System Boot</i>	17
Setting the CMOS Configuration	17
Bootting into Multiple Operating Systems	18

Using the Security Templates Snap-in to Secure Disk Resources 18

- Protecting Removable NTFS Media 18
- Restrict CDROM access to locally logged on user only 19
- Restrict Floppy access to locally logged on user only 19
- Disabling Media Autorun..... 19

Chapter 5 Backup and Recovery..... **21**

- Backups*..... 21
 - Security Implications 21
 - Auditing Backup and Restore Actions 22
- Recovery Procedures*..... 23
 - Emergency Repair Disk 23
 - Creating an Emergency Repair Disk..... 23
 - Recovering the System Using an Emergency Repair Disk..... 24
 - The Recovery Console 25

Appendix A References..... **27**

Table of Figures

Figure 1 - Audit Policy	14
Figure 2 - File Auditing	15

Table of Tables

Table 1 - Default Security Templates.....	4
Table 2 - File Permissions and Descriptions.....	5
Table 3 - Folder Permissions Options.....	6
Table 4 - File Permissions Options.....	7
Table 5 - Recommended File/Folder Permissions to add.....	8
Table 6 - Recommended Audit Policy Setting for File Events	14

Introduction

This guide is part of a series of guides related to securing the Windows 2000 operating system. Its purpose is to inform the reader about the available security settings for Windows 2000 file and disk resources, and how to properly implement those settings. This guide provides step-by-step instructions to perform many of the tasks recommended to secure files and directories. Application requirements may dictate that some settings differ from those recommended. If an application requires less restrictive settings, these exceptions should be documented.

The ***Guide to Securing Microsoft Windows 2000 File and Disk Resources*** presents detailed information on how to securely configure Access Control Lists (ACLs), file share permissions, file auditing, and backups. It will also address disk resource security and use of the Recovery Console.

This document is intended for Windows 2000 network administrators, but should be read by anyone involved or interested in Windows 2000 or network security.

Knowledge of Microsoft's Management Console (MMC) and the Security Configuration and Analysis Snap-in is assumed. Refer to the *Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Toolset* for detailed information on using snap-ins to securely configure a system.

Getting the Most from this Guide

This guide contains suggestions to successfully secure Windows 2000 file and disk resources.



WARNING: This document does not address site-specific issues. Every setting in this book should be tested on a non-operational network.

- ❑ Read this guide in its entirety. Subsequent chapters build on information and settings discussed in prior chapters. Omitting or deleting steps can potentially lead to an unstable system and/or network that will require reconfiguration and reinstallation of software.
- ❑ Perform pre-configuration recommendations:
 - Perform a complete backup of your system if this is not a new installation.
 - Install the Microsoft Windows NTFS file system on all partitions. NTFS is a requirement for implementing file security and configuring file auditing.
 - Apply the latest Windows 2000 service pack and security-related hotfixes.

About the Guide to Securing Microsoft Windows 2000 File and Disk Resources

This document consists of the following chapters:

Chapter 1, “Securing the Windows 2000 File System”, contains instructions for converting other file systems to Microsoft’s NTFS and configuring file ACLs securely.

Chapter 2, “Shared Resources”, contains detailed instructions and recommendations for setting share permissions on Windows 2000 File Resources.

Chapter 3, “File Auditing”, contains detailed instructions and recommendations for configuring the system to audit the use of Windows 2000 files.

Chapter 4, “Securing Disk Resources,” contains configuration recommendations for safeguarding disk resources.

Chapter 5, “Backup and Recovery”, presents recommendations for establishing a backup policy to safeguard against the loss of critical files as well as how to recover from system failure.

Appendix A, “References,” contains a list of resources cited.

Securing the Windows 2000 File System

Windows 2000 New Technology File System (NTFS) is a secure file system that provides a reliable way to safeguard valuable information. NTFS works in concert with the Windows 2000 user account system to allow authenticated users access to files.

The following notation will be used throughout this chapter:

%SystemDrive% - the drive letter on which Windows 2000 is installed, e.g. C:\

%SystemRoot% - the folder in which Windows 2000 is installed, e.g. C:\winnt

%SystemDirectory% - %SystemRoot%\system32, e.g. C:\winnt\system32

NTFS

All volumes must use NTFS in order to achieve the highest level of security. Under Windows 2000, only NTFS supports Discretionary Access Control to the directories and files. NTFS volumes provide secure and auditable access to the files. Therefore, any File Allocation Table (FAT16/FAT32) partitions should be converted to NTFS.

Windows 2000 introduces NTFS Version 5, which provides disk quotas and file encryption in addition to the features of previous NTFS versions. The Encrypting File System (EFS) is discussed in the *Guide to Securing Microsoft Windows 2000 Encrypting File System* mini-guide.

Converting to NTFS

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

The steps needed to convert a drive to NTFS are as follows:

- Select **Start**→**Run**→**cmd.exe** to open a command prompt
- At the command prompt, type:

```
convert volume /FS:NTFS [/V]
```



NOTE: Substitute the drive letter of the partition to be converted for *volume* (i.e. C:)



NOTE: The `/v` switch is optional and runs the program in verbose mode.

- Restart the system



NOTE: This conversion will not take effect immediately on the system drive or any drives being used for page swapping. In this case it is performed when the system is restarted. This process should not destroy any data.

Once the partition is converted, the Everyone group will have full control of the entire partition. Since the Everyone group consists of all users, including anonymous users (null connections), it is critical that stricter file permissions be set before any users are added to the system.

Default Security Templates

There are several security template files that contain the default security settings applied to a clean-installed (non-upgraded) Windows 2000 machine. These files reside in the %SystemRoot%\inf folder. **Table 1** shows a list of the default security templates.

The default security templates are especially useful when converting from a FAT or FAT32 file system to NTFS. To obtain the file system security settings that would have been present if NTFS had been the original file system, the File System portion of the default security templates can be applied. See Chapter 10 in the *Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Toolset* for more information on running the command-line utility `secedit.exe` and specifying that only the file system be configured.

File Name	Platform
Defltsv.inf	Windows 2000 Server/Advanced Server
Defltnk.inf	Windows 2000 Professional

Table 1 - Default Security Templates

File and Folder Permissions

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

To manually view permissions on a specific file or folder:

- In Windows Explorer right-click on the file or folder
- Select **Properties** from the pull-down menu
- Click the **Security** tab
- Click **Advanced** to see more detailed permission information

File permissions may be set with more granularity than those listed in the **Permissions** dialog box by clicking the **Advanced** button. **Table 2** shows a list of granular file permissions, and **Table 3** and **Table 4** show which granular permissions to select in order to achieve certain higher-level permissions for folders and files, respectively.

Special Permissions	Description
Traverse Folder/Execute File	Traverse Folder allows users to move through a folder to access other files or folders, regardless of permissions the user may or may not have on that folder (folders only). This permission only has meaning when the user has not been granted the Bypass Traverse Checking user right. The Execute File permission allows a user to run program files (files only).
List Folder/Read Data	List Folder allows the reading of file names and subfolders within a folder (folders only). Read Data allows file data to be read (files only).
Read Attributes	Allows viewing of a file's NTFS attributes (e.g. "Read only" or "Hidden").
Read Extended Attributes	Allows viewing of a file's extended attributes. Extended attributes may vary as they are defined by specific programs.
Create Files/Write Data	Create Files allows the creation of files within a folder (folders only). Write Data allows modification and/or overwriting of files (files only).
Create Folders/Append Data	Create Folders allows the creation of folders within a folder (folders only). Append Data allows making changes to the end of file (files only).
Write Attributes	Allows the modification of a file's NTFS attributes (e.g. "Read only" or "Hidden").
Write Extended Attributes	Allows the modification of a file's program-specific extended attributes.
Delete Subfolders and Files	Allows the deletion of subfolders and files regardless if the Delete permission was granted on the subfolder or file.
Delete	Allows deletion of a file or folder.
Read Permissions	Allows viewing of the permissions on a file or folder.
Change Permissions	Allows the modification of the permissions on a file or folder.
Take Ownership	Allows taking ownership of a file or folder.

Table 2 - File Permissions and Descriptions

Special Permissions	Full Control	Modify	Read & Execute	List Folder Contents	Read	Write
Traverse Folder/Execute File	x	x	x	x		
List Folder/Read Data	x	x	x	x	x	
Read Attributes	x	x	x	x	x	
Read Extended Attributes	x	x	x	x	x	
Create Files/Write Data	x	x				x
Create Folders/Append Data	x	x				x
Write Attributes	x	x				x
Write Extended Attributes	x	x				x
Delete Subfolders and Files	x					
Delete	x	x				
Read Permissions	x	x	x	x	x	x
Change Permissions	x					
Take Ownership	x					

Table 3 - Folder Permissions Options

NOTE: List Folder Contents is inherited by folders but not by files, while, Read and Execute is inherited by both folders and files.

Special Permissions	Full Control	Modify	Read & Execute	Read	Write
Traverse Folder/Execute File	x	x	x		
List Folder/Read Data	x	x	x	x	
Read Attributes	x	x	x	x	
Read Extended Attributes	x	x	x	x	
Create Files/Write Data	x	x			x
Create Folders/Append Data	x	x			x
Write Attributes	x	x			x
Write Extended Attributes	x	x			x
Delete Subfolders and Files	x				
Delete	x	x			
Read Permissions	x	x	x	x	x
Change Permissions	x				
Take Ownership	x				

Table 4 - File Permissions Options

Securing File and Folder Access Control Lists

Good file and folder security is critical in maintaining the overall security of a Windows 2000 system. Windows 2000 provides improved default file security over Windows NT 4.0, but additional file permissions are recommended to obtain a higher level of security.

The least privilege principle should be used when deciding how to implement ACLs. In other words, grant permissions to those users that need to have access and then allow those users only the access levels they absolutely require. For example, if a group needs Read access to a folder, resist the temptation to give the group Full control and only grant Read access.

Changes to file system ACLs can be made in one of two ways. The first method is to use the Microsoft Management Console (MMC) Security Templates snap-in and the provided template to apply the recommended file and folder permissions. The alternative and more time-consuming method is to manually change permissions on each file and folder.

The Security Templates snap-in is the recommended tool for creating a configuration file for setting security on Windows 2000 File Resources. See the *Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Toolset* for more information on using the Security Templates snap-in as well as adding, modifying, and excluding files and folders from the security policy. The recommended changes to system files and folders are also listed in the Security Configuration Toolset mini-guide.

To view file system settings using the Security Templates Snap-in do the following:

- In the **Security Templates** snap-in, select the default file directory (%SystemRoot%\Security\Templates)
- Select the specific configuration file
- Select **File System**

It is recommended that the folder(s) in **Table 5** be added to the security configuration template:


FOLDER OR FILE	USER GROUPS	RECOMMENDED PERMISSIONS
<p>%SystemRoot%\\$NtUninstall* (all uninstall folders) <i>folder, subfolders, and files</i></p> <p>Contains uninstall files for hotfixes and other applications.</p>  <p>NOTE: Substitute the name of the folder(s) for \$NtUninstall*. The security template will not recognize the wildcard character *.</p>	Administrators SYSTEM	Full Control Full Control

Table 5 - Recommended File/Folder Permissions to add

Additional File System Security Measures

Additional configuration changes and measures should be taken to further secure the Windows 2000 file system.

Removing the OS/2 and Posix subsystems

The OS2 and Posix subsystems in Windows 2000 can introduce security vulnerabilities to the operating system. Therefore, it is recommended that these subsystems be removed.

Deleting subsystem executables

Remove the following files from the following folders:

%SystemDirectory%\dllcache (%SystemRoot%\system32\dllcache)

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



NOTE: Windows 2000 has a facility called the System File Checker to detect changes to certain system modules in the %SystemDirectory%. It will automatically replace those modules with backup copies from the dllcache directory when they are changed or deleted.

%SystemDirectory%\ (%SystemRoot%\system32)

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

- psxdll.dll
- All Files in the \os2 folder, with the exception of the DLL folder and its contents.



NOTE: If the modules in the \DLL folder are removed, functions such as Cmd.exe will fail.

Deleting subsystem registry key values

Even if the subsystem executables have been removed, the subsystem could be reactivated if related registry keys still exist.

In addition to the above files, all registry keys related to the subsystems must be removed. Remove the following key values:

Hive: HKEY_LOCAL_MACHINE
 Key: \System\CurrentControlSet\Control\Session Manager\Environment
 Name: Os2LibPath
 Entry: Delete entry

Hive: HKEY_LOCAL_MACHINE
 Key: \System\CurrentControlSet\Control\Session Manager\Subsystems
 Name: Optional
 Entry: Delete entry

Hive: HKEY_LOCAL_MACHINE
 Key: \System\CurrentControlSet\Control\Session Manager\Subsystems
 Name: OS2 and POSIX
 Entry: Delete entries for both OS2 and POSIX

NOTE: Remove the actual key value listed under Name. Do not just blank out the string/number associated with the key value. Blanking out the string alone for the Optional value may result in a blue screen upon next system reboot.

Removing Leftover Directories on Upgraded Systems

When Windows 2000 is an upgrade to a Windows NT system, some obsolete directories are left on the system and should be deleted by the System administrator. These directories include, but may not be limited to:

- %SystemDrive%\DOS
- %SystemRoot%\Cookies
- %SystemRoot%\History
- %SystemRoot%\Temporary Internet Files

Preventing Data Remanence

Data remanence relates to images of data remaining on a Windows 2000 platform after the data should no longer be available. This includes data left in the system page file and the recycle bin. Each of these areas could have sensitive data that is open to being read by unauthorized or malicious users.

Recycle Bin

The Recycle Bin saves a copy of a file when it is deleted through Windows 2000 Explorer. On critical servers and key workstations, this could pose a security risk. A sensitive file may be deleted, yet a copy of that file would remain in the Recycle Bin. To configure the Recycle Bin to prevent deleted files from being saved, use the following procedure:

- Right click the **Recycle Bin** icon on the desktop, and select **Properties**.
- Check the box labeled “**Do not move files to the Recycle Bin. Remove files immediately on delete.**”
- Click **OK**.
- Empty the Recycle Bin of any pre-existing files.

System Page File

Virtual Memory support in Windows 2000 uses a system pagefile to swap pages from memory when they are not being actively used. On a running system, this pagefile is opened exclusively by the operating system and hence is well protected. However, to implement a secure Windows 2000 environment, the system page file should be wiped clean when Windows 2000 shuts down. This action ensures sensitive information, which may be in the page file, is not available to a malicious user.

To view file system settings using the Security Templates Snap-in do the following:

- Select the default file directory (%SystemRoot%\Security\Templates)
- Select the specific configuration file
- Select **Local Policies**
- Select **Security Options**
- Enable the setting for “**Clear virtual memory pagefile when system shuts down**”

Shared Resources

Windows 2000 shares are a means by which files, folders, printers, and other resources can be published for network users to remotely access. Regular users cannot create shares on their local machines; only Administrators and Power Users have this ability and must have at least List permission on the folder to do so. Since shares may contain important data and are a window into the local system, care must be taken to ensure proper security settings on shared resources.

The following share permissions can be granted or denied to users or groups:

- Full Control
- Change
- Read

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

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

Setting Share Permissions

To create a share and set security permissions:

- In explorer, right mouse-click on the folder that is to be shared.
- Select the **Sharing...** menu option
- Click the **Share this folder** radio button.
- Specify the **Share Name**.
- Click the **Permissions** button.
- Add, remove, or edit the users and/or groups in the access control list for the share.

Share Security Recommendations

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

- Ensure that the Everyone group is not given permissions on any shares.

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

Restricting anonymous listing of shares

To restrict the ability for anonymous logon users (also known as NULL session connections) to list account names and enumerate share names, using the Security Templates Snap-in do the following:

- ❑ Select the default file directory (%SystemRoot%\Security\Templates)
- ❑ Select the specific configuration file
- ❑ Select **Local Policies**
- ❑ Select **Security Options**
- ❑ Set **Additional restrictions for anonymous connections** to **No access without explicit anonymous permissions**.



WARNING: See the [Security Configuration Toolset mini-guide for information on potential problems caused by this setting](#).

File Auditing

File auditing is critical to maintaining file system security. Windows 2000 includes auditing capabilities that collect information about the use of file resources. For file auditing to function, system auditing must be enabled by configuring the auditing policy correctly.

Auditing Policy

On Windows 2000 systems, auditing is not enabled by default, and audit policies are set on a per-system basis via the Security Configuration Tool Set and the Security Templates snap-in. Each Windows 2000 system includes auditing capabilities that collect information about individual system usage. The logs collect information on applications, system, and security events. The three types of auditing are User Account, File System Auditing, and System Registry Auditing. Once System Auditing is configured, use the Security Templates snap-in to configure File Auditing. Windows 2000 Explorer can also be used to set File System Auditing.

Because of the importance of the Security Event Log in recording unauthorized accesses to the system, control of it should be limited to a select few. It is recommended that an “Auditors” group be created and given *Full Control* permissions to that log. Only individuals without administrator duties should be members of this group. This group should be given the User Right to “Manage auditing and security log” and the Administrators group should be removed from that right.



WARNING: Auditing can consume a large amount of processor time and disk space. It is highly recommended that administrators/auditors check, save, and clear audit logs daily/weekly to reduce the chances of system degradation or save audit logs to a separate machine. It is also recommended that logs be kept on a separate partition.

See the Security Configuration Toolset mini-guide for more information on setting audit policy.

Configuring Audit Policy for File Resources

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

To enable the audit policy setting to capture file events using the Security Templates Snap-in, do the following:

- ❑ Select the default file directory (%SystemRoot%\Security\Templates)
- ❑ Select the specific configuration file
- ❑ Select **Local Policies**→ **Audit Policy** (See **Figure 1**)
- ❑ Set **Audit Object Access** to enable auditing of failure events (see **Table 6**).

Auditing Policy Options	Recommended Settings
Audit Object Access Tracks attempts to access objects (directories, files, printers)	Failure

Table 6 - Recommended Audit Policy Setting for File Events

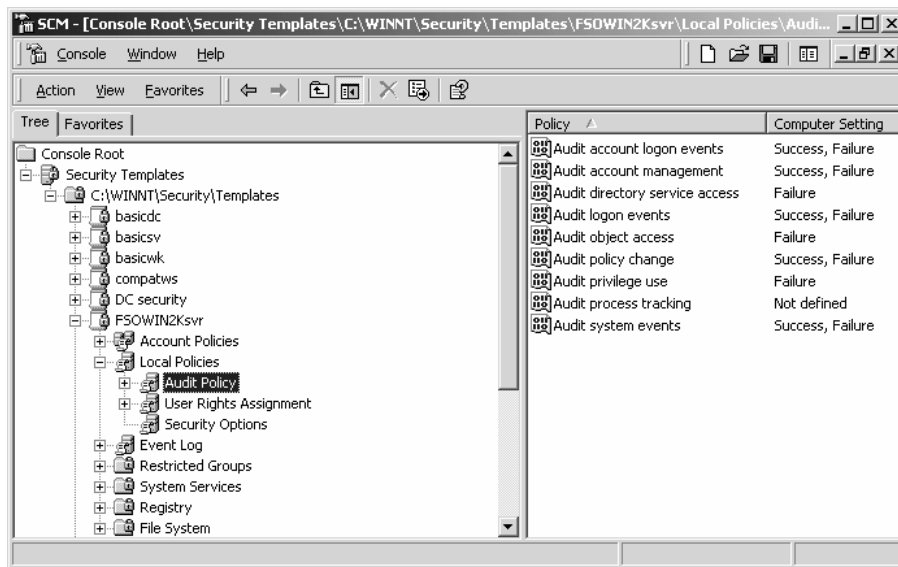


Figure 1 - Audit Policy

File Auditing

File System Auditing tracks a user's access to a specific directory or file. Auditing of sensitive files or directories may prove useful in identifying a system compromise or unauthorized use of resources.



NOTE: Like file permissions, file auditing can also be set via Windows 2000 Explorer or with the Security Templates MMC Snap-in.

To view file system settings using the Security Templates Snap-in so the following:

- Select the default file directory (%SystemRoot%\Security\Templates)
- Select the specific configuration file
- Select **File System**

Adding Audit Settings on a File or Folder

To add the audit settings on a particular file or folder through the Security Templates snap-in:

- In the right system object frame, double-click on the file or folder to be changed
- Ensure that the “**Replace existing permissions on all subfolders and files with inheritable permissions**” radio button is selected
- Click **Edit Security**
- Click the **Advanced** button.
- Select the Auditing tab.
- Uncheck the “**Allow inheritable auditing entries from parent to propagate to this object**” checkbox. Click on the **Remove** button in the **Security** dialog box.
- Click **Add** and select the group or user whose access will be audited
- Click **OK**.
- Select the desired audit settings. **Figure 2** shows a sample auditing scheme.

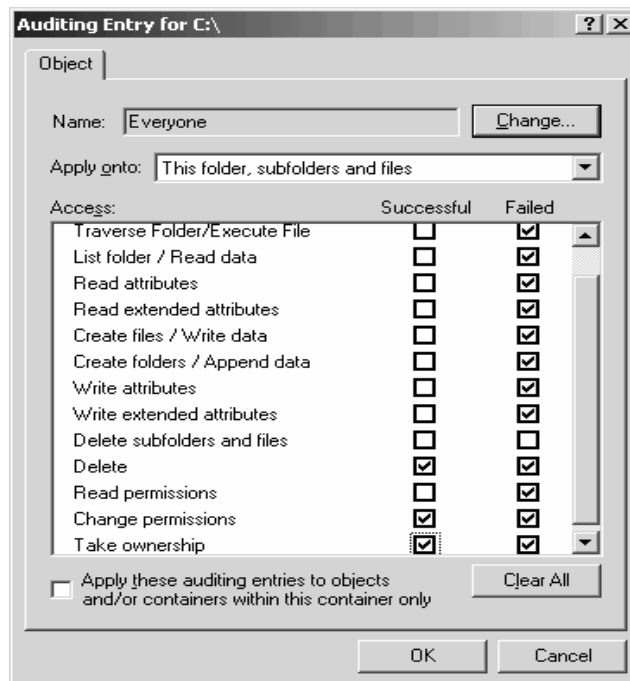


Figure 2 - File Auditing

- ❑ Click **OK**.
- ❑ Click **Apply**→**OK**→**OK**→**OK**

Modifying Audit Settings on a File or Folder

To modify the audit settings on a particular file or folder through the Security Templates snap-in:

- ❑ In the right frame, double-click on the file or folder to be changed
- ❑ Ensure that the “**Replace existing permissions on all subfolders and files with inheritable permissions**” radio button is selected
- ❑ Click **Edit Security**
- ❑ Click the **Advanced** button.
- ❑ Select the **Auditing** tab.
- ❑ Highlight the **Type** selection you want to modify.
- ❑ Click **View/Edit**.
- ❑ Edit the settings in the Audit Entry Window and click **OK**.
- ❑ Click **Apply**→**OK**→**OK**→**OK**

Securing Disk Resources

Disk resources include the physical hard drives and media of a computer system. To obtain a level of high security on a network, disk resources, in addition to operating system resources, must be protected.

Physical Security

Guidelines for protection of physical disk resources should be included in an organization's security policy. Physical security measures are needed to protect equipment and data from theft, corruption, and natural disasters. Therefore, controlling physical access to the resources is the first step.

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

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



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

Securing Disk Resources at System Boot

Setting the CMOS Configuration

Set boot options to prevent booting from removable media. This operation will vary from computer to computer, based on the manufacturer's specifications. During the initial boot sequence, **Press F1 to enter setup** will be displayed. (**F1** is only an example. Some systems use **F2**, **Ctrl/Del**, or **Ctrl/Esc**. Check the system's operating manual for specific details.)

- Set the computer CMOS to disallow removable media booting.

- ❑ Set the Password Configuration table as follows:
 - Supervisor Password **ON**
 - User Password **OFF**
- ❑ Set the CMOS Boot Password if necessary

When the option of defining which drives are bootable is not available in the system firmware, or the option to set a CMOS password is not available, set the CMOS Boot Password. This makes it more difficult for intentional or unintentional booting of the computer into a non-secure operating system.

Use procedures provided by the CMOS vendor. If necessary, upgrade the system CMOS chip.

During the initial boot sequence, press **F1** (or the required key sequence to enter system setup). Set the Password Configuration table as follows:

- ❑ Supervisor Password **ON**
- ❑ User Password **ON**

Use the Supervisor password for Administrators.



WARNING: Setting a power-on password will prevent a machine from rebooting in the event of a power failure.

Booting into Multiple Operating Systems

A Windows 2000 platform should be configured to prevent booting into other operating systems. The presence of less secure operating systems on the same platform could open disk resources to being manipulated by unauthorized users. Disk drives could be reformatted, or NTFS files could be copied or read using tools that are now available on the market.

Using the Security Templates Snap-in to Secure Disk Resources

The Security Templates snap-in can be used to set several disk resource security settings. A summary of these settings is provided below. See the Security Configuration Toolset mini-guide for more information.

Protecting Removable NTFS Media

By default, only Administrators can eject removable NTFS media from the computer. Ensure that this option has not been changed.

To view related disk resource system setting for this option using the Security Templates Snap-in do the following:

- ❑ Select the default file directory (%SystemRoot%\Security\Templates)
- ❑ Select the specific configuration file
- ❑ Select **Local Policies**
- ❑ Select **Security Options**

- ❑ Ensure that the policy “**Allowed to eject removable NTFS media**” is set to “**Administrators**”

Restrict CDROM access to locally logged on user only

By default, Windows 2000 allows any program to access files on CD-ROM drives. In a highly secure, multi-user environment, only allow interactive users to access these devices. When operating in this mode, the CD-ROM(s) are allocated to a user as part of the interactive logon process. These devices are automatically deallocated when the user logs off.

To view related disk resource system setting for this option using the Security Templates Snap-in do the following:

- ❑ Select the specific configuration file
- ❑ Select **Local Policies**
- ❑ Select **Security Options**
- ❑ Ensure that the policy “**Restrict CD-ROM access to the locally logged on user only**” is enabled



WARNING: Some software installation programs, including Microsoft's Installation Wizard allocate the CD-ROM under the System account. If “Restrict CD-ROM access to the locally logged on user only” is enabled, they will fail. Either disable this policy and reboot the machine to install the software, copy the installation files to the hard drive, or install from a network share. Enable this option again when the installation is complete.

Restrict Floppy access to locally logged on user only

By default, Windows 2000 allows any program to access files on floppy drives. In a highly secure, multi-user environment, only allow interactive users to access these devices. When operating in this mode, the floppy disks are allocated to a user as part of the interactive logon process. These devices are automatically deallocated when the user logs off.

To view related disk resource system setting for this option using the Security Templates Snap-in select the following:

- ❑ Select the specific configuration file
- ❑ Select **Local Policies**
- ❑ Select **Security Options**
- ❑ Ensure that the policy “**Restrict floppy access to the locally logged on user only**” is enabled

Disabling Media Autorun

Autoplay reads from a drive as soon as it is inserted. By default, Windows 2000 autoruns any CDROM that is placed in the drive. This could allow executable content to be run

without any access to the command prompt. Autoplay on floppy disks and network drives is disabled by default. A customized setting for disabling media autoplay has been added in the NSA security templates included with the *Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Toolset*. The options for this setting are:

- **CDROM drives** - disables autorun on CDROMs. Registry value = 0x00000095
- **All drives** - disables autorun on all media. Registry value = 0x000000FF

This option sets a value for the following registry key:

Hive: HKEY_LOCAL_MACHINE
 Key: \Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
 Name: NoDriveTypeAutoRun
 Entry: 0x95 (CDROM drives only) or 0xFF (all media)

To view related disk resource system setting for this option using the Security Templates Snap-in select the following:

- Select the specific configuration file
- Select **Local Policies**
- Select **Security Options**
- Ensure that the policy **Disable Media Autoplay** is set to **All drives**

NOTE: This option can also be set in Group Policy via Computer Configuration\Administrative Templates\System\Disable Autoplay. Because it is considered a security-related item, it has been added to the NSA security templates.

NOTE: CDROM autoplay/autorun can also be disabled by setting the registry value HKLM\System\CurrentControlSet\Services\Cdrom\Autorun = 0

Backup and Recovery

A disaster recovery plan is a critical part of any network's policy. This section describes recommended security practices for system backup and recovery.

Backups

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

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

Security Implications

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

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

There are several things to consider when preparing a backup policy:

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

Auditing Backup and Restore Actions

Users who have the right to backup and restore files and directories can gain access to sensitive files, even though file permissions may normally prevent them from doing so, by restoring them to a different location. Auditing the use of this user right gives security administrators the ability to identify suspicious file activity that may be outside of normal backup duties.

This setting determines whether to audit every use of user rights including **Backup** and **Restore**.

If you enable this policy, and if the **Audit privilege use** policy is enabled and in effect, then any instance of user rights being exercised will be recorded in the security log.

If you disable this policy, when users use **Backup** or **Restore** privileges, those events will not be audited even when **Audit Privilege Use** is enabled.



NOTE: This policy is defined by default in Local Computer Policy where it is disabled by default.



WARNING: This audit setting generates a large volume of audit events.

To enable the auditing of the use or user rights including Backup and Restore, use the Security Templates snap-in to do the following:

- Select **Security Templates**
- Select the default file directory (%SystemRoot%\Security\Templates)
- Specific configuration file
- Select **Local Policies**

- ❑ Select **Security Options**
- ❑ Enable the setting “**Audit use of Backup and Restore privilege**”



WARNING: Auditing of this privilege generates large volumes of data. Use caution if disk space is a concern.

Recovery Procedures

Emergency Repair Disk

The Emergency Repair Disk (ERD) feature helps you repair problems with system files, your startup environment, and the partition boot sector on your boot volume. Before you use the Emergency Repair Disk feature to repair your system, you must create an Emergency Repair Disk. You can do this using the Backup utility.

Even if you have not created an Emergency Repair Disk you can still try to use the Emergency Repair Disk process; however, any changes you have made to your system, such as Service Pack updates, may be lost and may need to be reinstalled.

Periodic updates of the ERD should be part of the standard operating procedures.

The ERD assists in recovery by:

- Repairing bad registry data
- Restoring corrupted or missing files on the system partition
- Replacing a corrupt Kernel, which is the core of the Windows 2000 operating system

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

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

Creating an Emergency Repair Disk

A blank formatted diskette is required when creating an ERD. To create the ERD:

- ❑ Insert a 3.5 inch, 1.44 MB floppy disk into the A: drive
- ❑ Select **Start** → **Programs** → **Accessories** → **System Tools** → **Backup**
- ❑ Select the **Emergency Repair Disk** button
- ❑ On the Emergency Repair Diskette window check “**Also backup the registry to the repair directory**”
- ❑ Click **Yes**
- ❑ Store the disk in a safe and secure place. It contains system security information that may be vulnerable to cracking.

Recovering the System Using an Emergency Repair Disk

The recovery process uses both the ERD and the original files from the Windows 2000 installation CD ROM. Consequently, the last Service Pack and all the previously installed hot fixes must be reinstalled after recovering with the ERD. The following steps provide a general overview of the emergency repair process:

- ❑ Start your computer from the Windows 2000 Setup disks or the CD
 - You can start your system using either the Windows 2000 Setup disks or the Windows 2000 CD. However, you can only use the CD to start your computer if your computer hardware and BIOS support this functionality.
- ❑ Choose the repair option during setup
- ❑ After your computer starts, the Setup program will start. During Setup you will be asked whether you want to continue installing the Windows 2000 operating system. You must press **ENTER** to continue. This will start the installation process, which allows you to repair your system.
- ❑ During this process you can choose whether you want to install a fresh version of Windows 2000, or whether you want to repair an existing installation of Windows 2000. To repair a damaged or corrupt system, you should press R.
- ❑ You will then be asked whether you want to repair your system using the Recovery Console or the emergency repair process. You should press R if you want to repair your system using the emergency repair process.
- ❑ Choose the type of repair
 - You can choose either the fast repair option, which is the easiest and doesn't require any user interaction, or you can choose the manual repair option, which requires user interaction. The fast repair option will attempt to repair problems related to the registry, system files, the partition boot sector on your boot volume, and your startup environment. The manual repair option lets you choose whether you want to repair system files, partition boot sector problems, or startup environment problems, but it doesn't let you repair problems with your registry.



NOTE: The manual repair option should only be used by advanced users or administrators.

The fast repair option will use a backup copy of the registry that was created when Setup was first run on your system. If you choose this option, you may lose settings or preferences you have created since Setup was first run.

If you want to manually repair individual registry files or replace your entire registry, you can use the Recovery Console. However, this is recommended for advanced users only.

- ❑ Start the repair process
 - To start the repair process, you should have the 1.44 MB ERD that you created in the Backup utility, and the original Windows 2000 installation CD. If you do not have an ERD, the emergency repair process can attempt to locate your Windows 2000 installation and start repairing your system, but it may not be able to do so.
- ❑ Restart your computer

If the emergency repair process was successful, your computer will automatically restart and you should have a working system.

The Recovery Console

The Windows 2000 Recovery Console provides a command line during startup from which you can make system changes when Windows 2000 doesn't start. Using the Recovery Console, you can start and stop services, format drives, read and write data on a local drive (including drives formatted to use NTFS), and perform many other administrative tasks. The Recovery Console is particularly useful if you need to repair your system by copying a file from a floppy disk or CD-ROM to your hard drive, or if you need to reconfigure a service that is preventing your computer from starting properly. Because the Recovery Console is quite powerful, you must be an administrator to use the Recovery Console.

Once you are running the Recovery Console, you can get help on the available commands by typing `help` at the command prompt.



NOTE: It is recommended that you back up your information before using Recovery Console. Your local hard drives may be formatted as part of the recovery.

There are two ways to start the Recovery Console:

- ❑ You can run the Recovery Console from your Windows 2000 Setup disks.
- ❑ You can install the Recovery Console on your computer to make it available in case you are unable to restart Windows 2000. You can then choose the **Windows 2000 Recovery Console** option from the boot menu.



NOTE: If Recovery Console isn't listed as a boot option, it is recommended that you install it to make it available as a startup option.

After starting the console:

- ❑ Choose which drive you want to log on to (if you have a dual-boot computer).
- ❑ Log on with your administrator password.



NOTE: Once you are running the Recovery Console, you can get help on the available commands by typing `help` at the command prompt.

UNCLASSIFIED

This Page Intentionally Left Blank

UNCLASSIFIED

References

Bartock, Paul, Julie Haney, et. al., *Guide to Securing Microsoft Windows NT Networks, Version 4.0*, National Security Agency, February 3, 2000.

DISA FSO, *Addendum to the Guide to Securing Microsoft Windows NT Networks, Version 1.3*, May 1, 2000.

Haney, Julie, *Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set, Version 1.0*, National Security Agency, May 2001.

Microsoft TechNet, <http://www.microsoft.com/technet>

Microsoft Windows 2000 Server Resource Kit, Group Policy Reference.

Microsoft Windows 2000 Server Resource Kit, Technical Reference to the Windows 2000 Registry.

Sjouwerman, Shilmover, and Stewart, *Windows 2000 System Administrator's Black Book*.