Windows NT Security

How To

Seminar

Wendall H. Mayson
wendall.mayson@srs.gov
(803)208-3438

John C. Cox
johnc.cox@srs.gov
(803)952-4743

Westinghouse Savannah River Company

WSRC-MS-97-0297

April 28, 1997

Table Of Contents

1. BRIEF OVERVIEW

A. What's This All About

Windows NT is a network operating system that will more than likely play an increasing role in the future of computing within the Department of Energy. In fact, Windows NT may already be the dominant network operating system at your site, or at least have a very large presence. For this reason, those of us involved in computer security must become familiar with Windows NT and the security features it offers.

This seminar was designed as a "How To" for Windows NT Security. We will attempt to present a short overview of Windows NT and the components of its Security Model. After that, we will provide some instructions on how to:

- setup a Windows NT Domain
- setup a Legal Warning Notice
- secure Windows NT objects and audit access to those objects
- review audit records
- setup Alerts
- create user accounts
- setup the user Rights Policy
- create groups
- setup the Account Policy
- create a User Profile

In addition, we will provide some information on Logon Scripts, auditing tools, and where you can go for additional information on Windows NT and specifically Windows NT security.

B. Windows NT

Although it will run on a PC platform, Windows NT is a big departure from the previous PC-based operating systems (e.g. DOS) and PC-based network operating systems (e.g. LAN Manager). Windows NT is a 32-bit, preemptive multitasking network operating system. It will run on both Complex Instruction Set Computing (CISC) processors and Reduced Instruction Set Computing (RISC) Processors. In fact, Windows NT was first implemented on a RISC chip. Microsoft implemented this by separating the portions of Windows NT that are machine specific into what is called the Hardware Abstraction Layer (HAL). This allows other or future types of processors to be supported by writing a new HAL. In addition, the Windows

NT kernel supports Symmetric Multiprocessors (SMP). The standard retail version of Windows NT Server 4.0 will support up to four processors and support for up to 32 processors is available from some hardware vendors. Windows NT Workstation will support two processors.

Version 3.51 of Windows NT has the familiar Windows 3.x interface and version 4.0 has the Windows 95 interface. The operating system includes compatibility with other operating systems, file systems, and networks. Windows NT is compatible with a number of network protocols including TCP/IP, IPX/SPX. NetBEUI, AppleTalk, DLC, SNA, and PPP.

There are two flavors of Windows NT, Windows NT Workstation and Windows NT Server. There are a number of similarities between workstation and server and they do share a lot of code (in fact the core system files are the same). The biggest difference is in the components that each includes. For example, NT Server includes network services such as Dynamic Host Configuration Protocol (DHCP), Domain Name Service (DNS), and Windows Internet Name Service (WINS) that NT Workstation lacks. NT Server version 4.0 also includes Microsoft FrontPage and Internet Information Server (IIS). One other major difference is the way in which the two flavors run software. NT Workstation provides the current foreground application the highest priority which gives the user's current application the most processor time. NT Server provides network services the highest priority. Also, the NT Workstation scheduler uses short timeslices while NT Server uses long timeslices.

If you have read any articles about Windows NT, it is pretty much assured that security was addressed. That's because security, along with networking, is a fundamental component of Windows NT. When Microsoft designed Windows NT, security was a design goal of the operating system. Security was then built into the core of the operating system. System administrators will find that security is pervasive throughout the operating system.

There are a tremendous number of security features in Windows NT. However, these features were not designed such that they are obtrusive. Windows NT includes a comprehensive set of tools to assist in managing and maintaining security. These GUI tools have the same look and feel as the other administrative programs provided in Windows NT. In addition, there are a number of third party products available as discussed later in this session. System administrators can utilize these tools to implement a security policy for their system that will protect their users and data, but at the same time not hinder users from getting their job done.

C. Windows NT Security Model

The Windows NT Security Model includes the following four components:

1. Logon Process – The Logon Process accepts logon requests from users. Logon requests include interactive logons from local users and network logons from remote users.

2. Local Security Authority - The Local Security Authority (LSA) is also referred to as the Windows NT security subsystem. The LSA is responsible for the following:
    a) Generating access tokens (Access tokens are generated for a user when they logon. The access token is a user's "security badge" and includes a security ID for the user. Windows NT uses the security ID to determine if a user has the required permissions or rights needed when the user attempts to access an object.)
    b) Managing the local security policy
    c) Providing interactive user authentication services
    d) Controlling the audit policy and logs audit messages

3. Security Account Manager - The Security Account Manager (SAM) maintains the user accounts database. The user accounts database contains data for all users and groups. The SAM processes validates requests from the LSA.

4. Security Reference Monitor - The Security Reference Monitor enforces object access validation and audit generation rules defined by the LSA. The Security Reference Monitor contains the only copy of the access validation code which ensures that objects are protected uniformly throughout the operating system. The Security Reference Monitor provides the following services:

    a) Validating access to objects
    b) Testing users for privileges
    c) Generating audit messages

The Windows NT Security Model was designed to regulate access to objects (the Windows NT definition of objects is described later). The security model maintains security data for each user, group, and object. This data is used to validate access attempts that are made by a user or on behalf of the user by another process. The security model also tracks and logs the access attempts.

D. C2 Security And Windows NT

Windows NT has been evaluated by the National Computer Security Center (NCSC) and the base operating system has been rated C2 under the "Orange

Book" criteria. The initial evaluation was for Windows NT version 3.5, but version 4.0 has been placed on the NCSC maintenance program.

The networking portion of Windows NT is under evaluation by the NCSC. The networking portion is being evaluated under the criteria defined in the "Red Book".

The Windows NT Resource Kit offers a very useful utility called C2 Config. This utility can be very helpful in setting up Windows NT to be C2 compliant or for checking compliance with the C2 requirements.

2. WORKGROUP MODEL VS. DOMAIN MODEL

A. Overview

With Windows NT a system can be setup on a network as a member of a workgroup or a member of a domain. Workgroups and domains can be thought of as organizational units on a network. The decision on whether to use the Workgroup Model or the Domain Model will depend on a number of variables including:

- Number of systems involved.
- The logical grouping of users (e.g., departmental).
- Quantity of resources the systems will need to share (shared resources are defined below).
- Whether or not a server is available to support a domain.
- How much security is required.
- How knowledgeable the users are.

The above list is not all-inclusive and network administrators will have to evaluate their individual situations when determining which model to use.

B. Workgroups

A workgroup, as defined by Microsoft, is a collection of systems that are grouped for viewing purposes. In this case, viewing means users on other systems, in the workgroup, would be able to "see" or view the systems in the workgroup and the shared resources being served by systems in the workgroup. Shared resources would be any portion of a system such as a disk drive or printer that can be used by users on other systems in the workgroup.

Systems in a workgroup individually manage their own user and group account information and their own security and account policy databases. Resources being shared by a system in a workgroup are also individually managed. The best use of the workgroup configuration is for small groups of systems with few users, or where the network is configured without an NT Server.

There can be one to many systems in a workgroup. In addition, there can be multiple workgroups on a network and each workgroup would have a unique name. One final note, systems in a workgroup would NOT belong to a domain.

As mentioned above, workgroups are best used for small groups of systems. Once the number of systems increases beyond a few, the administration of each individual one can become a hassle. Since all security and resource sharing must

be setup and administered on each individual system, versus on a single server in a domain, a workgroup can quickly become unmanageable.

C. Domains

A domain is a collection of systems, servers and workstations that are grouped together. The systems in a domain share a domain directory database which includes a single security policy and user account database (SAM database) that is maintained by the domain system administrator. Centralizing the user account database and security policy provides the domain system administrator with an easy and effective way to maintain the security policies across the network for all systems. For the users, it provides an effective, secure, and easy way to access all shared resources in the domain with a single logon.

Domains consist of a Primary Domain Controller (PDC) and one or more Backup Domain Controllers (BDC). A domain controller is a server that manages/maintains the domain directory database and manages all aspects of domain user interactions such as authenticating users logging into domain accounts. The PDC is responsible for tracking any changes made to accounts for all systems in the domain. It is the only domain controller to receive changes directly. A domain has only one PDC. A BDC receives a copy of the domain's directory database from the PDC. The copy is periodically and automatically synchronized between the master copy on the PDC and the copy maintained on the BDC. A BDC can authenticate users and can be promoted to function as the PDC should the PDC crash or be taken out of service.

The decision of whether or not an Windows NT server will be a domain controller must be made during operating system installation. During installation, the system administrator will be asked if the server will function as a domain controller. **This is an irreversible decision!** The only way to change a server's function from domain controller to non-domain controller (or vice versa) is to reinstall the operating system.

Designating a server to be the primary domain controller (PDC) is the first step in creating a Windows NT Domain. If the system administrator specifies that the system will be a domain controller, a domain name will be required. This name must be unique on the network.

Additional systems can be added to the domain in one of the following ways:

1. Additional Windows NT Servers that will function as Backup Domain Controllers (BDC) are added during operating system installation on the respective servers. Simply specify the same domain name that was used on the PDC.

2. Windows NT workstations and Windows NT servers (not functioning as domain controllers) are added via the Network applet in Control Panel. If the system is already a member of another domain, specify the new domain name. If the system is a member of a workgroup, specify that the system will be a member of a domain and specify the domain name.
3. Systems can also be added and removed using the Server Manager utility under Administrative Tools on Windows NT server.

A valid domain administrator user ID and password is required to add a system to a domain.

D. Trust Relationships

Trust relationships are a way to simplify administration of a network consisting of multiple Windows NT domains. A trust relationship allows a user to have a single account in one domain and be able to access resources in one or many other domains. In addition, trust relationships allow system administrators to manage multiple domains from a single location.

A trust relationship is a link between domains in which one domain will honor the users of another domain. Trust relationships consist of a trust*ing* domain and a trust*ed* domain. The trusting domain will recognize the user accounts and global groups established on the trusted domain. The user accounts on the trusted domain can be added to the local groups and assigned permissions and rights in the trusting domain.

The link between domains is both an administrative link (the establishment of the relationship) and a communications link (the "pass-through" validation of users). Pass-through validation occurs when a user account must be authenticated and the system being used for logon validation is not the domain controller that holds the account. In this case, the system (in the trusting domain) being used for logon validation would pass the authentication request to the appropriate domain controller (in the trusted domain) for validation.

There are two types of trust relationships, a one-way trust and a two-way trust. In a one-way trust, only one domain (trusting domain) trusts the other (trusted domain). In a two-way trust, both domains trust each other. It is possible to have multiple trust relationships between several domains. For example, many domains can trust a domain where all accounts are maintained in a single location or a single domain could trust multiple domains in which accounts are spread out. The first example would be the most secure implementation of trust relationships due to the central administration of user accounts.

E. Types Of Domain Models

The following are the four types of Domain Models:

- Single Domain
  The Single Domain is the best model for organizations with a small number of users (fewer than 10,000) and only a few resources. There is only one domain in this model; therefore, there is no administration of trust relationships. Administration of user accounts is centralized, and global groups are used for accessing resources.

- Master Domain
  The Master Domain model includes multiple domains, with one being the master domain. The master domain is trusted by all other resource/organizational domains, but does not trust any of them nor do the resource/organizational domains trust each other. This model provides the benefits of centralized administration of multiple domains.

  In the Master Domain model, administration of user accounts and organizational resources are in separate domains. Resources are managed locally on the trusting domains, while user accounts are controlled on the trusted master domain. The master domain model is used in organizations with less than 10,000 users. The number of users is limited because the accounts are all maintained on the master domain.

- Multiple-Master Domain
  The Multiple Master Domain model is used for organizations with computer resources grouped into logical divisions, such as by departments or location. This model is identical to the Master Domain model except that there is more than one master domain. All master domains have a two-way trust with each other. Each resource/organizational domain trusts all master domains, but the resource/organizational domains do not trust each other. Since the master domains trust each other and the resource/organizational domains trust the master domains, every user account can access resources in each of the domains. This model is designed for organizations with more than 10,000 users.

- Complete-Trust Domain
  The Complete-Trust (sometimes referred to as the Multiple Trust) model supports multiple domains that all trust each other. Administration of this model is very complex due to the lack of control over the user accounts and groups in all domains. If the organization has a large number of domains, there will be a very large number of trust relationships to manage. This model can support up to 10,000 users per domain. Each domain has total control over its own user accounts.

  Administration of this model is decentralized and is not practical for organizations desiring structured account management. Each administrator of a domain depends on the administrators of the other domains to correctly

manage their users and groups. This would include not allowing improper users into global groups that have access to sensitive information.

This model is not recommended because of the lack of security and the high volume of administration.

3. NT LOGON PROCESS

A. Overview

Logging on to a Windows NT system or domain is similar to most other operating systems in that a username and password is required. Two unique features are present in the Windows NT world, however. First, logon is initiated by pressing the Control, Alt, and Delete keys simultaneously (**CTRL-ALT-DELETE**) as if to warm boot an IBM compatible system. Rather than reboot, Windows NT intercepts this non-maskable interrupt (NMI) and begins the logon process. If the same **CTRL-ALT-DELETE** key combination is pressed while logged on, a control window will pop up allowing locking of the workstation with a screen saver and other options. The second unique feature of the Windows NT logon process is that a drop-down **FROM** box is provided to choose between logging onto the domain or logging onto the local workstation.

During the Windows NT logon process, the user account information (User ID and Password) are passed to the Security Account Manager (SAM) for validation. If the account information correctly corresponds to an account in the user account database, the Local Security Authority (LSA) constructs an access token for the user and a process is started (see Section 1.C.). If the account information is incorrect, the system returns the message "User Authorization Failure."

A word of warning: The **CTRL-ALT-DELETE** key combination helps protect against applications running in the background (e.g. application-level Trojan horse programs) that might be used to intercept passwords. It is still possible, however, to create a device-driver-based or DOS-based Trojan horse program to intercept passwords. Proper system set up, auditing, and physical protection (especially for systems with bootable floppy disk drives) can greatly reduce this sort of threat.

B. Password Selection

As in other operating systems, selection of a hard-to-guess password is at the core of user security management. Minimum password lengths, lifetime of passwords, and password histories can easily be set up in Windows NT (see Section 12). Windows NT passwords **are case sensitive**, may be up to 14 characters in length, and can include characters, numbers, and punctuation except the following:

- " / \ [ ] : ; | = , + * ? < >

Unfortunately, Windows NT does not currently provide a random password generator function within the operating system. A separate password generation program can be provided, and the user instructed to only use generated passwords. The user must still be trusted to actually use a generated password, typing it into the appropriate input box when changing passwords. This means that the generation program should be as painless as possible to increase the chance that users will comply.

A simple GUI-based program (e.g. Visual Basic) that provides pseudo-pronounceable passwords can be provided to aid in this process.

C. Legal Warning Notice

Many sites require that computer logon screens include a legal warning about proper system use, penalties for misuse, notice of auditing, etc. Windows NT provides a capability to present the user with a legal warning screen after **CTRL-ALT-DEL** is pressed, but before the logon screen is presented. The legal warning consists of a dialog box with caption (title), warning text, and an **OK** button. The legal warning is controlled by two registry entries:

Warning Caption

HKEY_LOCAL_MACHINE\SOFTWARE
\Microsoft\Windows NT\CurrentVersion
\Winlogon\LegalNoticeCaption

Warning Text

HKEY_LOCAL_MACHINE\SOFTWARE
\Microsoft\Windows NT\CurrentVersion
\Winlogon\LegalNoticeText

D. How To Setup A Legal Warning Notice

1. Open the Registry Editor and select the **HKEY_LOCAL_MACHINE** window.
2. Double-click on the **SOFTWARE** folder.
3. Double-click on the **MICROSOFT** folder.
4. Double-click on the **WINDOWS NT** folder.
5. Double-click on the **CURRENTVERSION** folder.
6. Double-click on the **WINLOGON** folder.
7. Double-click on the **LEGALNOTICECAPTION** key.
8. Enter text for the title of the legal notice dialog box and click on **OK**.
9. Double-click on the **LEGALNOTICETEXT** key.
10. Enter text for the body of the legal notice dialog box and click on **OK**.
11. Exit the Registry Editor.

Unfortunately, carriage returns cannot be directly entered in the LegalNoticeText key. This makes for rather ugly legal notices if a lot of text is required. One workaround is to enter text normally, inserting a unique character wherever a carriage return is desired (e.g. ~). Determine the hexadecimal value of the unique character (e.g. hex 7E for ~), then use the binary mode of the registry key editor to change the unique character's code to a hex 0D (carriage return).

The more elegant and flexible method is to use the REGINI.EXE command-line utility from the Windows NT Resource Kit. REGINI takes a specially formatted text file and directly enters values in the registry. It can be used to change many registry keys to predetermined values quickly and consistently. Follow the instructions provided in the Resource Kit.

Note: Third-party logon utilities may disable the legal warning notice, even if the registry keys are properly set. In particular, the Novell 32-bit NDS client for NT will defeat the legal warning notice settings.

4. FILE AND DIRECTORY CONTROLS

A. Overview

One of the key objectives of the Windows NT Security Model is to control access to objects. Files and directories are considered by Windows NT to be objects and the terms are used interchangeable throughout this section. Using the NT File System (NTFS), object owners can control which users or groups of users can access which objects and how the objects may be accessed. Object owners and system administrators can assign permissions to users and groups that either grant or deny access to an object. This ability to assign permissions at the discretion of the owner or system administrator is called discretionary access control (DAC). DAC is a requirement for an operating system to be C2 certified by the NCSC.

Windows NT implements DAC through the use of Access Control Lists (ACL) and Access Control Entries (ACE). ACLs can contain from zero to many ACEs. An ACL is created for each object on the system. When an object owner or system administrator assigns a permission to a user or group for an object, an ACE is created and inserted into the ACL. The ACL can be thought of as a container for ACEs. The ACEs hold the security information for the object that describes the specific access permissions that have been granted for a particular user or group.

Users set object permissions through File Manager or Windows NT Explorer.

Note: Microsoft added Windows NT Explorer to Windows NT 4.0. Explorer is another utility that can be used to work with files and directories. The old File Manager is still available although it is not added to the Start menu by default in Windows NT 4.0.

B. Object Permission Tables

The following tables, which can be found in Appendix A, provide a list of the permissions that may be assigned to objects:

- Table 1 - A list and description of the basic permissions that may be assigned to files.
- Table 2 - A list and description of the custom permissions that may be assigned to files when the basic permission “Special Access” is selected.
- Table 3 - A list and description of the basic permissions that may be assigned to directories.

- Table 4 - A list and description of the custom permissions that may be assigned to directories when the basic permission "Special Directory Access" is selected.
- Table 5 - A list and description of the permissions for directories and their effects on files.
- Table 6 - A list and description of the permissions that may be assigned to shared directories.
- Table 7 - Permission Abbreviations
- Table 8 - A list and description of the permissions that may be assigned to Registry keys and subkeys.
- Table 9 - A list and description of the permissions that may be assigned to printers.

C. How To Assign Permissions To Files And Directories

To assign permissions on files and directories:

1. Open File Manager and select the appropriate file or directory.
2. Click the Security icon (a key) or from the **SECURITY** menu choose **PERMISSIONS.** The **FILE/DIRECTORY PERMISSIONS** dialog box appears.
3. Select the users or groups whose permissions you wish to change, select the appropriate permission from the **TYPE OF ACCESS** drop down box, and click **OK**. You may also click the **REMOVE** button to remove access for the users or groups selected.
4. To add access for a user or group, click the **ADD** button and the **ADD USERS AND GROUPS** dialog box appears. From the **LIST NAMES FROM** drop down box select the local system or domain whose user accounts database contains the users or groups you wish to add access for. Select the users (click the **SHOW USERS** button to display users) and groups you wish to add (if you select a group, you can click the **MEMBERS** button to see a list of users and global groups that are members of the selected group). Click the **ADD** button, select the appropriate permission from the **TYPE OF ACCESS** drop down box and click **OK** to return to the **FILE/DIRECTORY PERMISSIONS** dialog box.
5. Once you have made all necessary changes, click **OK** to return to the File Manager.

   Notes: If you select the permission **SPECIAL ACCESS**, an additional dialog box appears to allow you to select the Special Access permissions you wish to assign. Once you have made your selections, click **OK** to return to the **FILE/DIRECTORY PERMISSIONS** dialog box.

   When assigning permissions to a directory, two check boxes are available to allow you to: 1) **REPLACE PERMISSIONS ON SUBDIRECTORIES**; and 2) **REPLACE PERMISSIONS ON FILES.** By default, permissions you set on a directory are applied to the directory and any files in the directory. Select the first check box to apply permissions to all subdirectories also. Clear the

second check box if you want the permissions applied to the directory only.

To assign permissions on files and directories using Explorer in Windows NT 4.0:

1. Open Explorer and select the appropriate file or directory.
2. Right click the mouse and choose **PROPERTIES** or from the **FILE** menu choose **PROPERTIES**. The **PROPERTIES** dialog box appears.
3. From the **PROPERTIES** dialog box select the **SECURITY** tab and click the **PERMISSIONS** button. The **FILE/DIRECTORY PERMISSIONS** dialog box appears.
4. Select the users or groups whose permissions you wish to change, select the appropriate permission from the **TYPE OF ACCESS** drop down box, and click **OK**. You may also click the **REMOVE** button to remove access for the users or groups selected.
5. To add access for a user or group, click the **ADD** button and the **ADD USERS AND GROUPS** dialog box appears. From the **LIST NAMES FROM** drop down box select the local system or domain whose user accounts database contains the users or groups you wish to add access for. Select the users (click the **SHOW USERS** button to display users) and groups you wish to add (if you select a group, you can click the **MEMBERS** button to see a list of users and global groups that are members of the selected group). Click the **ADD** button, select the appropriate permission from the **TYPE OF ACCESS** drop down box and click **OK** to return to the **FILE/DIRECTORY PERMISSIONS** dialog box.
6. Once you have made all necessary changes, click **OK** to return to the **PROPERTIES** dialog box. Click **OK** again to return to Explorer.

Note: The default permissions for the root directory of an NTFS partition are:

- Administrators - Full Control
- Creator Owner - Full Control
- Everyone - Change

D. File Management

Through proper file management, system administrators and object owners can usually control access or permissions at the directory level instead of the file level. It is obviously much easier to assign permissions to a single directory than to the hundreds or possibly thousands of files in the directory. Of course, there will always be special cases where permissions will need to be assigned to individual files and in those cases it is appropriate. System administrators should practice good file management techniques and should instruct their users to do so as well.
Some suggestions are:

- Don't allow users to create directories and place files all over the place. Assign users a default directory and force them to put their directories and files there.
- In group situations, assign the group leader the permissions necessary to create high level directories to ensure there is control.
- Users have a tendency to keep everything. Encourage them to keep only what is really needed and if they really want to hang on to their old files, archive them to removable media.
- Always group files by categories and place them in directories. Develop a scheme for the files that you have on your system, and then develop a directory structure to match your scheme.
- Perform regular backups, both incremental and full, and rotate tapes (e.g. use the son, father, grandfather method).
- Keep backups in a secure location remote from the system.

Good security starts with and depends on good system administration, and good file management is a key ingredient to a well-managed system.

E. Shared Directories

Shared (over the network) directories are the only directories where permissions can be set regardless of the file system being used. However, the permissions set are only applicable when the directory is accessed through the share name (that is, accessed via the network). If the shared directory is on an NTFS formatted partition, the permissions assigned on the individual objects are also in effect. The permissions assigned to a share apply to the shared directory and all subdirectories and files in it.

F. How To Assign Permissions On Shared Directories

To assign permissions on a shared directory:

1. Open File Manager and select the directory being shared or to be shared.
2. Click the Share icon (a hand holding a solid folder) or from the **DISK** menu choose **SHARE AS**. The **SHARED DIRECTORY** or **NEW SHARE** dialog box appears depending on whether or not the directory has been previously shared.
3. Click the **PERMISSIONS** button. The **ACCESS THROUGH SHARE PERMISSIONS** dialog box appears.
4. Select the users or groups whose permissions you wish to change, select the appropriate permission from the **TYPE OF ACCESS** drop down box, and click **OK**. You may also click the **REMOVE** button to remove access for the users or groups selected.

5. To add access for a user or group, click the **ADD** button and the **ADD USERS AND GROUPS** dialog box appears. From the **LIST NAMES FROM** drop down box select the local system or domain whose user accounts database contains the users or groups you wish to add access for. Select the users (click the **SHOW USERS** button to display users) and groups you wish to add (if you select a group, you can click the **MEMBERS** button to see a list of users and global groups that are members of the selected group). Click the **ADD** button, select the appropriate permission from the **TYPE OF ACCESS** drop down box and click **OK** to return to the **FILE/DIRECTORY PERMISSIONS** dialog box.
6. Once you have made all necessary changes, click **OK** to return to the **SHARED DIRECTORY** or **NEW SHARE** dialog box. Click **OK** again to return to the File Manager.

To assign permissions on shared directory using Explorer in Windows NT 4.0:

1. Open Explorer and select the directory being shared or to be shared.
2. Right click the mouse and choose **PROPERTIES** or from the **FILE** menu choose **PROPERTIES**. The **PROPERTIES** dialog box appears.
3. From the **PROPERTIES** dialog box select the **SHARING** tab and click the **PERMISSIONS** button. The **FILE/DIRECTORY PERMISSIONS** dialog box appears.
4. If the directory is not currently being shared, select the **SHARE AS** option.
5. Click the **PERMISSIONS** button. The **ACCESS THROUGH SHARE PERMISSIONS** dialog box appears.
6. Select the users or groups whose permissions you wish to change, select the appropriate permission from the **TYPE OF ACCESS** drop down box, and click **OK**. You may also click the **REMOVE** button to remove access for the users or groups selected.
7. To add access for a user or group, click the **ADD** button and the **ADD USERS AND GROUPS** dialog box appears. From the **LIST NAMES FROM** drop down box select the local system or domain whose user accounts database contains the users or groups you wish to add access for. Select the users (click the **SHOW USERS** button to display users) and groups you wish to add (if you select a group, you can click the **MEMBERS** button to see a list of users and global groups that are members of the selected group). Click the **ADD** button, select the appropriate permission from the **TYPE OF ACCESS** drop down box and click **OK** to return to the **FILE/DIRECTORY PERMISSIONS** dialog box.
8. Once you have made all necessary changes, click **OK** to return to the **PROPERTIES** dialog box. Click **OK** again to return to Explorer.

G. File Ownership

The creator of a file or directory is by default the owner. The owner can not give someone ownership, but they can assign permission to a user or group to take

ownership. To take ownership of an object, a user or group must have the Full Control permission or the Special Access permission Take Ownership on the object. In addition, the system administrator can take ownership or grant a user or group the Take ownership of files or other objects right. File ownership is only supported on an NTFS partition.

H. How To Take Ownership Of Files And Directories

To take ownership of a file or directory:

1. Open File Manager and select the file or directory.
2. From the **SECURITY** menu choose **OWNER**. The **OWNER** dialog box appears.
3. Click the **TAKE OWNERSHIP** button. If you have selected a directory to take ownership of, Windows NT will notify you that you have selected a directory and ask if you would like to also take ownership of all the files and subdirectories contained in the selected directory. Answer accordingly.

To take ownership of a file or directory using Explorer in Windows NT 4.0:

1. Open Explorer and select the file or directory.
2. Right click the mouse and choose **PROPERTIES** or from the File menu choose **PROPERTIES**. The **PROPERTIES** dialog box appears.
3. From the **PROPERTIES** dialog box select the **SECURITY** tab and click the **OWNERSHIP** button. The **OWNER** dialog box appears.
4. Click the **TAKE OWNERSHIP** button. If you have selected a directory to take ownership of, Windows NT will notify you that you have selected a directory and ask if you would like to also take ownership of all the files and subdirectories contained in the selected directory. Answer accordingly. The **PROPERTIES** dialog appears.
5. Click **OK** to return to Explorer.

I. Important Things To Remember About File And Directory Controls

- Each ACE will either grant or deny some access to an object. A deny ACE is always placed in the ACL higher than a grant ACE (Note: This can be altered by third-party products or locally-developed software which may place certain grant ACEs ahead of deny ACEs, so BEWARE). When Windows NT checks permissions in the ACL it starts at the top and scans down the list. If a deny access ACE is found, the checking is stopped and access is denied.
- Grant ACEs are cumulative. For example, if user John has Read access to a file and the group Payroll, which John is a member of, has Write access to the same file, then John has Read + Write access to that file.
- By default, files inherit permissions from their parent directory.

- You must use NTFS. DAC is not supported under the File Allocation Table (FAT) file system or the High-Performance File System (HPFS). Note: HPFS is only supported on Windows NT versions prior to 4.0.
- If a file has an ACL with no ACEs, no access has been granted and any access requested will be denied. Therefore, by not granting a user or group any permissions to a particular object, you deny them any access by default.
- Users or groups granted the Full Control permission on a directory can delete files in the directory regardless of the permissions assigned to the individual files.
- Establishing permissions for groups of users instead of each individual user is a much more effective way for system administrators to implement file and directory controls. Please review the topic Group Management in Section 11 for additional information on utilizing groups in Windows NT.
- When a file is copied it inherits permissions from the directory into which it is copied.
- When a file is moved it retains its existing permissions.

J. Files and Directory Access Auditing

System administrators can enable auditing for files and directories stored on NTFS partitions. For each file or directory selected for auditing, the system administrator can define users and/or groups to be audited and the type of access or event to audit. The available events are:

- Read
- Write
- Execute
- Delete
- Change Permissions
- Take Ownership

For each auditable event, the system administrator can choose to audit successes and/or failures. For example, if the system administrator wanted to know each and every time someone attempted to read a file, he would enable success and failure auditing for the Read event. This would ensure that each time someone attempted to open the file for read access, whether they were successful or not, an audit record would be written to the Security Event Log (see Security Event Log Topic in Section 7).

Note: In order to perform file and directory access auditing, the audit policy for the system must be enabled and the File and Object Access event must be enabled accordingly. In addition, the following registry value should be added:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Lsa
\FullPrivilegeAuditing
Type is REG_BINARY

Value is 1

K. How To Enable File And Directory Auditing

To enable file and directory auditing:

1. Open File Manager and select the appropriate file or directory.
2. From the **SECURITY** menu choose **AUDITING**. The **FILE/DIRECTORY AUDITING** dialog box appears.
3. Select the users or groups whose auditing status you wish to change, and then enable or disable the appropriate **SUCCESS** or **FAILURE** check boxes for the events. You may also click the **REMOVE** button to disable auditing for the users or groups selected.
4. To add auditing for a user or group, click the **ADD** button and the **ADD USERS AND GROUPS** dialog box appears. From the **LIST NAMES FROM** drop down box select the local system or domain whose user accounts database contains the users or groups you wish to add auditing for. Select the users (click the **SHOW USERS** button to display users) and groups you wish to add (if you select a group, you can click the **MEMBERS** button to see a list of users and global groups that are members of the selected group) and click the **ADD** button. Once you have made your selections, click the **OK** button to return to the **FILE/DIRECTORY AUDITING** dialog box. Select each of the users and groups added and enable or disable the appropriate **SUCCESS** or **FAILURE** check boxes for the events.
5. Once you have made all necessary changes, click **OK** to return to the File Manager.

   Note: When enabling auditing on a directory, two check boxes are available to allow you to: 1) **REPLACE AUDITING ON SUBDIRECTORIES**; and 2) **REPLACE AUDITING ON EXISTING FILES**. By default, auditing you enable on a directory is applied to the directory and any files in the directory. Select the first check box to enable auditing on all subdirectories also. Clear the second check box if you want auditing enabled on the directory only.

To enable file and directory auditing using Explorer in Windows NT 4.0:

1. Open Explorer and select the appropriate file or directory.
2. Right click the mouse and choose **PROPERTIES** or from the File menu choose **PROPERTIES**. The **PROPERTIES** dialog box appears.
3. From the **PROPERTIES** dialog box select the **SECURITY** tab and click the **AUDITING** button. The **FILE/DIRECTORY AUDITING** dialog box appears.
4. Select the users or groups whose auditing status you wish to change, and then enable or disable the appropriate **SUCCESS** or **FAILURE** check boxes for the events. You may also click the **REMOVE** button to disable auditing for the users or groups selected.

5. To add auditing for a user or group, click the **ADD** button and the **ADD USERS AND GROUPS** dialog box appears. From the **LIST NAMES FROM** drop down box select the local system or domain whose user accounts database contains the users or groups you wish to add auditing for. Select the users (click the **SHOW USERS** button to display users) and groups you wish to add (if you select a group, you can click the **MEMBERS** button to see a list of users and global groups that are members of the selected group) and click the **ADD** button. Once you have made your selections, click the **OK** button to return to the **FILE/DIRECTORY AUDITING** dialog box. Select each of the users and groups added and enable or disable the appropriate **SUCCESS** or **FAILURE** check boxes for the events.
6. Once you have made all necessary changes, click **OK** to return to the **PROPERTIES** dialog box. Click **OK** again to return to Explorer.

L. A Few Words About Reviewing Audit Records

It is possible for a system administrator to become overwhelmed by file auditing. Determining which files to audit on larger systems can become a real chore. Some suggestions are:

- Ask group leaders which of their files contain sensitive data and should be audited.
- Where possible, only audit failed access attempts.
- Audit important system files. The registry files, Event Log files, and User Profiles are all stored in WINNT\SYSTEM32\config.
- Audit access to Logon Scripts (see the Logon Script topic in Section 14).
- Where possible, audit at the directory level instead of auditing individual files. Turn on auditing for the directory and propagate the auditing down to the subdirectories and files as explained above.

5. REGISTRY CONTROLS

A. Overview

The Registry is a database in Windows NT used for storing information about a system's configuration. Some of the information stored in the Registry includes installed hardware and settings, installed software, installed network protocols, environment settings, security settings, and user information.

The Registry is made up of keys, subkeys, and value entries. A collection of keys, subkeys, and value entries is called a hive. Keys and subkeys are analogous to directories and subdirectories, and value entries are analogous to files.

Like files and directories, items in the Registry are considered objects by Windows NT and permissions can be assigned to them. However, permissions for the Registry can only be assigned to keys and subkeys and not value entries. Permissions can be assigned in the Registry regardless of the type of file system being used.

B. Some Suggested Settings

When Windows NT is installed, the group Everyone is given write access to a great deal of the Registry. Therefore, it is obvious that a system administrator will want to make some changes in order to better secure the system. Listed below are some changes that can be reviewed for possible implementation:

1. In File Manager, place permissions on REGEDT32.EXE to prevent users from running the Registry Editor program. Note: REGEDT32.EXE is the executable program for the Registry Editor. By default, Windows NT does not install a separate program item for this program. However, it can be accessed through the File Manager, Explorer, the Run command, and Windows NT Diagnostics (prior to Windows NT version 4.0)
2. Prevent remote Registry access. This can be accomplished by adding the following Registry key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ SecurePipeServers\winreg. Note that this key is present by default in Windows NT Server 4.0, but must be added on Windows NT Workstation 4.0, Windows NT Server 3.51, and Windows NT Workstation 3.51.
3. System administrators may remove the permission for the group Everyone at HKEY_LOCAL_MACHINE. Do not select **REPLACE PERMISSION ON EXISTING SUBKEYS** and be aware that this may cause problems with some applications.

As discussed in Part C below, ensure auditing is turned on so the change can be monitored.

C. A Warning

Assigning permissions in the Registry can be very risky because it is easy to restrict access to a key or subkey that an application needs to access in order to run. In fact, Microsoft recommends that you only assign permissions on keys and subkeys that have been added to support custom applications or settings.

Before making any changes to the security of the Registry, turn on auditing and monitor the Security Event Log for failed access attempts to the keys or subkeys whose permissions were modified (see Registry Access Auditing topic below). This will give some indication of whether or not the incorrect users have been locked out. In addition, it will let the system administrator know if unauthorized users are snooping. Review the logs carefully; it may be that the permissions assigned just need to be modified and not all security dropped. In other words, instead of changing the permission from no access to full control, it might be changed to read. System administrators should also set permissions such that the groups Administrators and System have full control. This will ensure that the system will at least boot and a user in the Administrator group can correct any permissions incorrectly changed.

D. How To Assign Permissions In The Registry

To assigned permissions in the Registry:

1. Open the Registry Editor and select the appropriate key or subkey.
2. From the **SECURITY** menu choose **PERMISSIONS**. The **REGISTRY KEY PERMISSIONS** dialog box appears.
3. Select the users or groups whose permissions you wish to change, select the appropriate permission from the **TYPE OF ACCESS** drop down box, and click **OK**. You may also click the **REMOVE** button to remove access for the users or groups selected.
4. To add access for a user or group, click the **ADD** button and the **ADD USERS AND GROUPS** dialog box appears. From the **LIST NAMES FROM** drop down box select the local system or domain whose user accounts database contains the users or groups you wish to add access for. Select the users (click the **SHOW USERS** button to display users) and groups you wish to add (if you select a group, you can click the **MEMBERS** button to see a list of users and global groups that are members of the selected group). Click the **ADD** button, select the appropriate permission from the **TYPE OF ACCESS** drop down box and click **OK** to return to the **REGISTRY KEY PERMISSIONS** dialog box.

5. Once you have made all necessary changes, click **OK** to return to the Registry Editor.

Notes: If you select the permission **SPECIAL ACCESS**, an additional dialog box appears to allow you to select the special access permissions you wish to assign. Once you have made your selections, click **OK** to return to the **REGISTRY KEY PERMISSIONS** dialog box.

A check box is available to allow you to **REPLACE PERMISSIONS ON EXISTING SUBKEYS.** When this box is checked, the assigned permissions will be replaced on the selected key and all of its subkeys.

Table 8 provides a list and description for the permissions that may be assigned to Registry keys and subkeys.

E. Registry Access Auditing

System administrators can enable auditing for Registry keys and subkeys. For each key or subkey selected for auditing, the system administrator can define users and/or groups to be audited and the type of access or event to audit. The available events are:

- **QUERY VALUE** - system activity that attempts to read a value entry from a key.
- **SET VALUE** - system activity that attempts to set value entries in a key.
- **CREATE SUBKEY** - an attempt to create subkeys on a key.
- **ENUMERATE SUBKEYS** - any event that attempts to identify the subkeys of a key.
- **NOTIFY** - notification event from a key.
- **CREATE LINK** - events that attempt to create a symbolic link in a particular key
- **DELETE** - attempts to delete key.
- **WRITE DAC** - an attempt to gain access to a key to write an ACL (assigning a permission).
- **READ CONTROL** - attempt to access the security assigned to a key.

In addition, for each auditable event, the system administrator can choose to audit either successes or failures. For example, if the system administrator wanted to know each and every time someone attempted to delete the SOFTWARE subkey or any of its subkeys, he would enable success and failure auditing for the **DELETE** event and check the **AUDIT PERMISSIONS ON EXISTING SUBKEYS** box as described below. This would ensure that each time someone attempted to delete the SOFTWARE subkey or any of its subkeys, whether they were successful or not, an audit record would be written to the Security Event Log (see Security Event Log Topic in Section 7).

Note: In order to perform Registry access auditing, the audit policy for the system must be enabled and the File and Object Access event must be enabled accordingly. In addition, the following registry value should be added:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Lsa
\FullPrivilegeAuditing
Type is REG_BINARY
Value is 1

F. How To Enable Registry Access Auditing

To enable Registry auditing:

1. Open Registry and select the appropriate key or subkey.
2. From the **SECURITY** menu choose **AUDITING**. The **REGISTRY KEY AUDITING** dialog box appears.
3. Select the users or groups whose auditing status you wish to change, and then enable or disable the appropriate **SUCCESS** or **FAILURE** check boxes for the events. You may also click the **REMOVE** button to disable auditing for the users or groups selected.
4. To add auditing for a user or group, click the **ADD** button and the **ADD USERS AND GROUPS** dialog box appears. From the **LIST NAMES FROM** drop down box select the local system or domain whose user accounts database contains the users or groups you wish to add auditing for. Select the users (click the **SHOW USERS** button to display users) and groups you wish to add (if you select a group, you can click the **MEMBERS** button to see a list of users and global groups that are members of the selected group) and click the **ADD** button. Once you have made your selections, click the **OK** button to return to the **REGISTRY KEY AUDITING** dialog box. Select each of the users and groups added and enable or disable the appropriate **SUCCESS** or **FAILURE** check boxes for the events. If you wish for the selected events to be applied to all of the subkeys for the selected key or subkey, check the **AUDIT PERMISSIONS ON EXISTING SUBKEYS** box.
5. Once you have made all necessary changes, click **OK** to return to the Registry Editor.

6. PRINTER CONTROLS

A. Overview

As with Files and Directories, system administrators can control access to printers by assigning permissions. When a permission is assigned, Access Control Entries (ACEs) are placed in the Access Control List (ACL) for the printer. Table 9 provides a list and description of the permissions that may be assigned to printers.

Access to printers may need to be controlled for a number of reasons. For example, if a printer is in an unrestricted area, the system administrator may want to prevent certain groups of users, who normally print sensitive information, from using it. Also, certain departments may want to restrict who can use their printer especially if it is in high demand or costs a great deal to use (a color laser for example).

Setting permissions on a printer also allows the system administrator to let certain users manage the printer and relieve him of that task. If a printer is setup for a particular department, someone in that department can be assigned the necessary permissions to manage the print jobs sent to the printer.

Permissions for printers are set in the **SECURITY** menu in the Print Manager for Windows NT versions prior to 4.0, or in the **PRINTER PROPERTIES** for Windows NT 4.0.

B. How To Assign Permissions To Printers

To assign permissions on printers from Print Manager:

1. Open Print Manager and select the appropriate printer.
2. From the **SECURITY** menu choose **PERMISSIONS**. The **PRINTER PERMISSIONS** dialog box appears.
3. Select the users or groups whose permissions you wish to change, select the appropriate permission from the **TYPE OF ACCESS** drop down box, and click **OK**. You may also click the **REMOVE** button to remove access for the users or groups selected.
4. To add access for a user or group, click the **ADD** button and the **ADD USERS AND GROUPS** dialog box appears. From the **LIST NAMES FROM** drop down box select the local system or domain whose user accounts database contains the users or groups you wish to add access for. Select the users (click the **SHOW USERS** button to display users) and groups you wish to add (if you select a group, you can click the **MEMBERS** button to see a list of users and global groups that are members of the selected group). Click the **ADD** button, select the

appropriate permission from the **TYPE OF ACCESS** drop down box and click **OK** to return to the **PRINTER PERMISSIONS** dialog box.

5. Once you have made all necessary changes, click **OK** to return to the Print Manager.

To assign permissions on Printers in Windows NT 4.0:

1. Click on the **START** button and from the **SETTINGS** menu select **PRINTERS**.
2. Right click the mouse on the appropriate printer and choose **PROPERTIES** or click on the appropriate printer to select it and from the **FILE** menu choose **PROPERTIES**. The **PROPERTIES** dialog box appears.
3. From the **PROPERTIES** dialog box select the **SECURITY** tab and click the **PERMISSIONS** button. The **PRINTER PERMISSIONS** dialog box appears.
4. Select the users or groups whose permissions you wish to change, select the appropriate permission from the **TYPE OF ACCESS** drop down box, and click **OK**. You may also click the **REMOVE** button to remove access for the users or groups selected.
5. To add access for a user or group, click the **ADD** button and the **ADD USERS AND GROUPS** dialog box appears. From the **LIST NAMES FROM** drop down box select the local system or domain whose user accounts database contains the users or groups you wish to add access for. Select the users (click the **SHOW USERS** button to display users) and groups you wish to add (if you select a group, you can click the **MEMBERS** button to see a list of users and global groups that are members of the selected group). Click the **ADD** button, select the appropriate permission from the **TYPE OF ACCESS** drop down box and click **OK** to return to the **PRINTER PERMISSIONS** dialog box.
6. Once you have made all necessary changes, click **OK** to return to the **PROPERTIES** dialog box. Click **OK** again to return to the Desktop.

C. How To Take Ownership Of Printers

To take ownership of a printer using Print Manager:

1. Open Print Manager and select the appropriate printer.
2. From the **SECURITY** menu choose **OWNER**. The **OWNER** dialog box appears.
3. Click the **TAKE OWNERSHIP** button.

To take ownership of a printer in Windows NT 4.0:

1. Click on the **START** button and from the **SETTINGS** menu select **PRINTERS**.
2. Right click the mouse on the appropriate printer and choose **PROPERTIES** or click on the appropriate printer to select it and from the **FILE** menu choose **PROPERTIES**. The **PROPERTIES** dialog box appears.
3. From the **PROPERTIES** dialog box select the **SECURITY** tab and click the **OWNERSHIP** button. The **OWNER** dialog box appears.

4. Click the **TAKE OWNERSHIP** button.
5. Click **OK** to return to the Desktop.

D. Printer Access Auditing

System administrators can audit the success or failure of a user's attempts to:

- Print documents.
- Change the settings of print jobs.
- Pause or restart print jobs.
- Reorder print jobs.
- Delete print jobs.
- Share printers.
- Remove printers.
- Add, remove, or change permissions set on a printer.
- Change a printer's owner.

Note: In order to perform printer access auditing, the audit policy for the system must be enabled and the File and Object Access event must be enabled accordingly. In addition, the following registry value should be added:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Lsa
\FullPrivilegeAuditing
Type is REG_BINARY
Value is 1

E. How To Enable Printer Access Auditing

To enable printer auditing:

1. Open Print Manager and select the appropriate printer.
2. From the **SECURITY** menu choose **AUDITING**. The **PRINTER AUDITING** dialog box appears.
3. Select the users or groups whose auditing status you wish to change, and then enable or disable the appropriate **SUCCESS** or **FAILURE** check boxes for the events. You may also click the **REMOVE** button to disable auditing for the users or groups selected.
4. To add auditing for a user or group, click the **ADD** button and the **ADD USERS AND GROUPS** dialog box appears. From the **LIST NAMES FROM** drop down box select the local system or domain whose user accounts database contains the users or groups you wish to add auditing for. Select the users (click the **SHOW USERS** button to display users) and groups you wish to add (if you select a group, you can click the **MEMBERS** button to see a list of users and global groups that are members of the selected group) and click the **ADD** button. Once you have made your selections, click the **OK** button to return to the **PRINTER AUDITING** dialog box. Select each of the users and groups added and

enable or disable the appropriate **SUCCESS** or **FAILURE** check boxes for the events.

5. Once you have made all necessary changes, click **OK** to return to the Print Manager.

To enable printer auditing in Windows NT 4.0:

1. Click on the **START** button and from the **SETTINGS** menu select **PRINTERS.**
2. Right click the mouse on the appropriate printer and choose **PROPERTIES** or click on the appropriate printer to select it and from the **FILE** menu choose **PROPERTIES**. The **PROPERTIES** dialog box appears.
3. From the **PROPERTIES** dialog box select the **SECURITY** tab and click the **AUDITING** button. The **PRINTER AUDITING** dialog box appears.
4. Select the users or groups whose auditing status you wish to change, and then enable or disable the appropriate **SUCCESS** or **FAILURE** check boxes for the events. You may also click the **REMOVE** button to disable auditing for the users or groups selected.
5. To add auditing for a user or group, click the **ADD** button and the **ADD USERS AND GROUPS** dialog box appears. From the **LIST NAMES FROM** drop down box select the local system or domain whose user accounts database contains the users or groups you wish to add auditing for. Select the users (click the **SHOW USERS** button to display users) and groups you wish to add (if you select a group, you can click the **MEMBERS** button to see a list of users and global groups that are members of the selected group) and click the **ADD** button. Once you have made your selections, click the **OK** button to return to the **PRINTER AUDITING** dialog box. Select each of the users and groups added and enable or disable the appropriate **SUCCESS** or **FAILURE** check boxes for the events.
6. Once you have made all necessary changes, click **OK** to return to the **PROPERTIES** dialog box. Click **OK** again to return to Desktop.

7. SECURITY EVENT LOG

A. Overview

Once File and Directory, Registry, and Printer Access Auditing have been enabled, Windows NT will generate an audit record each time an event occurs which matches an enabled event. Each audit record generated is written to the Security Event Log.

B. How To Review Audit Records

To review audit records generated for File and Directory, Registry, and Printer Access Auditing:

1. Open the Event Viewer. If the Security Log is not currently being displayed, from the **LOG** menu select **SECURITY**.
2. From the **VIEW** menu select **FILTER EVENTS**. The **FILTER** dialog box appears.
3. Select the **VIEW FROM** and **VIEW THROUGH** dates and times for the appropriate time period.
4. Select the **TYPES** of audit records to display.
5. In the **SOURCE** drop down list, select **SECURITY**.
6. In the **CATEGORY** drop down list select **OBJECT ACCESS**.
7. Additional filtering can also be set for a particular User, Computer, or Event ID. (Note: Any significant occurrence in Windows NT, an application being run that requires a user to be notified, or a record to be written to a log file is considered by Windows NT to be an event. Each event is assigned a numeric value that is considered its ID.)
8. Once you have set the desired filtering options, click **OK** to return to the Event Viewer. The audit records that meet the filter options are listed.
9. To view a more detailed description of a particular record, either:
   - Select the record and from the **VIEW** menu select **DETAIL**
   - Select the record and hit the **ENTER** key
   - Double click on the record.

   The Event Detail dialog box appears.

C. Log Settings

System administrators can and should increase the default size of the Security Event Log. The default size of the log is 512K. In addition, the administrator can select their preferred log wrapping options. The available options are to overwrite events as needed, overwrite events older than a defined number of days, and do

not overwrite any events. In the case of the latter option, the system administrator will have to clear the log manually.

To set options for the Security Event Log:

1. Open the Event Viewer and from the **LOG** menu select **LOG SETTINGS**. The **EVENT LOG SETTINGS** dialog box appears
2. If the Security Log is not selected, use the drop down box to change to it.
3. Change the maximum log size to what is appropriate for your system (the appropriate size for your system will depend on a number of variables such as the number of users you have and the amount of auditing turned on).
4. Select the appropriate **EVENT WRAPPING OPTION.**
5. Once you have selected the appropriate option, click **OK** to return to the Event Viewer.

D. One Important Registry Setting

To ensure that no security related auditable events are lost, system administrators will want to enable CrashOnAuditFail. CrashOnAuditFail is a Windows NT registry entry that will force the operating system to shutdown. The full path for the registry entry is:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
\CrashOnAuditFail

There are two possible values for this entry.

1 Will force the system to shutdown if the Security Event Log is full

2 This value will be set by Windows NT just before it crashes. While the entry is set to 2, only administrators can logon.

Note: There is no 0 value for this entry, to disable CrashOnAuditFail remove the entry from the registry.

To restore the system after a forced shutdown, the system administrator would logon, and archive the events in the Security Event Log to free up space. In addition, the value in the registry would need to be changed from 2 back to 1.

8. ALERTS

A. Overview

Alerts are an administrative tool that can be used by system administrators to warn them about security-related events. When an alert is generated by the system a message can be sent to a defined list of users and systems. In addition, the system administrator can choose to have a program run the first time or every time a specified Alert occurs. The Alerter and Messenger services must be started on the system where the alerts will be originating from and the Messenger service must be started on any systems defined to receive alert messages. Alerts will be sent when the established limit of a counter is reached.

Some good security related counters, under the Server object, are:

- **Errors Access Permissions** - The number of times opens on behalf of clients have failed with STATUS_ACCESS_DENIED. Can indicate whether somebody is randomly attempting to access files in hopes of getting at something that was not properly protected.
- **Errors Granted Access** - The number of times accesses to files was denied. Can indicate attempts to access files without proper access authorization.
- **Errors Logon** - The number of failed logon attempts to the server. Can indicate whether password-guessing programs are being used to crack the security on the system.
- **Errors System** - The number of times an internal Server Error was detected. Could indicate a problem with the system.
- **Logon Total** - Includes all interactive logons, network logons, service logons, successful logon, and failed logons since the system was last rebooted.
- **Logon/sec** - Logon/sec is the rate of all logons.
- **Sessions Forced Off** - The number of sessions that have been forced to logoff. Can indicate how many sessions were forced to logoff due to logon time constraints.
- **Sessions Timed Out** - The number of sessions that have been closed due to their idle time exceeding the autodisconnect parameter for the system.

From the Alert Log, system administrators can monitor the counters that have been added. If a counter reaches the established limit, an event is recorded in the Alert Log. The Alert Log can record 1000 events, after which the oldest event will be dropped when a new one is received. If the system administrator in not viewing the Alert Log when an Alert occurs, an Alert Icon appears.

B. How To Set An Alert

To Set an Alert

1. Open the Performance Monitor and from the **VIEW** menu choose **ALERT**. The Performance Monitor will change to the **ALERT LOG** view.
2. From the **EDIT** menu choose **ADD TO ALERT**. The **ADD TO ALERT** dialog box appears.
3. Select the **SERVER** object from the **OBJECT** drop down box.
4. Select the appropriate counter from the **COUNTER** drop down box. Click the **EXPLAIN** button to get a description of the counter.
5. In the **ALERT IF** box choose **OVER** or **UNDER** (for security related events select **OVER**) and then enter an appropriate number.
6. If a program should run when a specified Alert occurs, in the **RUN PROGRAM ON ALERT** box type the full path of the program and select whether it should run the **FIRST TIME** or **EVERY TIME** the Alert occurs.
7. For **SERVER** objects, there is no need to worry about the **INSTANCE** box.
8. Click the **ADD** button and then either setup another Alert or click the **DONE** button to close the **ADD TO ALERT** dialog box.
9. From the **OPTIONS** menu choose **ALERT**. The **ALERT OPTIONS** dialog box appears.
10. Choose the appropriate options to occur when an Alert occurs. A single option or a combination of options may be set. In addition, a time interval may be set for updates to the Alert Log or the Log may be updated manually. If **MANUAL UPDATE** is selected, the Log can be updated by choosing **UPDATE NOW** from the **OPTIONS** menu for the Performance Monitor **ALERT LOG** view.
11. Click the **OK** button to return to the **ALERT LOG** view in the Performance Monitor.

9. USER ACCOUNT MANAGEMENT

A. Overview

The User Manager in Windows NT Workstation or User Manager For Domains in Windows NT Server, is the administrative tool for managing user accounts, groups, and the security policies associated with users. A Windows NT user account contains information about a specific user including, but not limited to, the username, password, groups the user is a member of, and the rights the user has been granted. In Windows NT, a group is essentially an account containing user accounts and in some case groups. A user in a group is a member of the group.

Included in the User Manager Policy menu is the Account Policy and User Rights Policy, which are used for managing user account security policies. The Account Policy is used to control password characteristics such as password length and password age. The User Rights Policy is used to view or change the rights that are granted to a user or group. Each of the above topics is addressed in more detail below.

Accounts must be established for all users who need to logon to a Windows NT system, with two exceptions. Windows NT establishes an Administrator account and a Guest account when it is installed.

B. Administrator Account

The Administrator account has control over the entire system including its operation and security. This is the most powerful account on the system and is established for the system administrator to use. The Administrator account can not be deleted, but it can be renamed (see Note below). It is recommended that this account be renamed because it is a known account that could be used by a hacker. One other property of the Administrator account is that it can not be disabled. This property has been established to prevent a denial of service attack and ensures that one account, with administrator rights, is always available for use provided the password is available. Therefore, the password for the Administrator account must not be forgotten. If the Administrator account is the only available account with administrator rights and the password is unavailable, Windows NT must be reinstalled to restore the system (there are vendors who provide a password recovery service for a fee if you wish to try such a service).

Note: Since Windows NT identifies/validates users by their Security Identifier (SID), any account can be renamed. SIDs are unique for every user and are never reused by Windows NT.

System administrators and other users who do system administration should each have two accounts on the system. One account should be a member of the Administrator group and the other account should be a general user account for general or normal system work. This is to avoid making mistakes such as changing the permissions on objects that should not be changed. In addition, if a user was logged on as an administrator and activated a program that contained a virus, the damage to the system could be much more severe because the virus would have all of the permissions and rights of the system administrator.

C. Guest Account

The Guest account is established for logon by users who may need to logon one time or very infrequently. The account is disabled by default on Windows NT Server and enabled by default on Windows NT Workstation. The Guest account is established with a blank password and may be used for both local and network logons.

The Guest account can not be deleted, but it can be renamed. If the account is to be used, it should be renamed and given a non-trivial password. In addition, if it is to be used infrequently, it should only be enabled when needed. Even though the Guest account is "non-privileged", it is still an account on the system with some basic permissions and rights. For example, Guest account users would have access to any objects the group Everyone (see discussion of Special Groups Topic in Section 11) is given permission to access or have any rights the group Everyone is granted. System administrators should evaluate the permission and rights granted to the Guest account and the group Everyone on a regular basis. In addition, system administrators should regularly evaluate groups the Guest account is a member of.

D. How To Create A New Account

To create a new account:

1. Open User Manager and from the **USER** menu choose **NEW USER**. The **NEW USER** dialog box appears.
2. Enter the following information for the new user in the appropriate box:
   a) their logon username or account name,
   b) the user's real name,
   c) a description for the user,
   d) the users initial password,
   e) reenter the initial password for confirmation.
3. Select the appropriate properties for the new user:

A) **USER MUST CHANGE PASSWORD AT NEXT LOGON.** Checked by default. When selected, this property forces the user to change their password from the one assigned by the system administrator when the account was created.

B) **USER CANNOT CHANGE PASSWORD.** This is selected by default for the Guest account only. The Guest account is probably the only account where this property should be selected.

C) **PASSWORD NEVER EXPIRES.** This is selected by default for the Guest account only. The Guest account is probably the only account where this property should be selected. Selecting this property overrides the Maximum Password Age setting in the Account Policy and the account property User Must Change Password at Next Logon.

D) **ACCOUNT DISABLED.** This property is used to disable an account. System administrators can utilize this property to disable accounts (such as the Guest account) that will not be used for an extended period of time.

4. Click on the **GROUPS** button. The **GROUP MEMBERSHIPS** dialog box appears. Select the groups the user is not a member of but should be and click the **ADD** button. Select the groups the user is a member of but should not be and click the **REMOVE** button. When you are finished, click **OK** to return to the **NEW USER** dialog box. Note: Group Management is discussed in more detail later in this section.
5. Click on the **PROFILE** button. The **USER ENVIRONMENT PROFILE** dialog box appears. Enter the following information as desired or necessary:
   a) The path where the user's profile is stored. This can be in the form of a network path.
   b) The name of the file for the user's logon script. Note: If the logon script file is located in a subdirectory of the system's default logon script path (normally WINNT\SYSTEM32\imports\scripts), you must include the path prior to the filename. For example, if the script file is in a subdirectory called managers, it would be written as "manager\mgrlogon.bat.
   c) For the **HOME DIRECTORY**, you may specify a path for a local directory on a workstation or a network path on a server. When you are finished, click OK to return to the New User dialog box. Note: User profiles and logon scripts are discussed in more detail later in this section.
6. Click on the **HOURS** button. The **LOGON HOURS** dialog box appears. By default users can logon all hours. To make a change, select the hours to be disallowed by dragging the cursor over the desired blocks and clicking the **DISALLOW** button. This can be reversed by selecting the desired blocks and clicking the **ALLOW** button. An entire day can be selected by clicking on the desired day's button or certain hours can be selected for all seven days by clicking the button at the top of the chart for the desired hours. When you are finished, click **OK** to return to the **NEW USER** dialog box.

7. Click on the **LOGON FROM** button. The **LOGON WORKSTATIONS** dialog box appears. By default users can logon to any workstation. To restrict the workstations the user can use, select **USER MAY LOG ON TO THESE WORKSTATIONS** and enter up to a maximum of eight workstation names. When you are finished, click **OK** to return to the **NEW USER** dialog box.
8. Click on the **ACCOUNT** button. The **ACCOUNT INFORMATION** dialog box appears. From this box an account expiration date can be established and the **ACCOUNT TYPE** can be selected.
   a) To establish an account expiration date, select **END OF** and enter the appropriate date. At the end of the day for the date entered the account will be disabled (not deleted).
   b) Select the appropriate **ACCOUNT TYPE**. Global accounts are for normal users or users within the system's domain. These users are allowed to logon interactively to systems within the domain (unless disallowed as described above) and their accounts can be used in domains that have a trust relationship with their domain. Local accounts are for users whose regular account (or Global account as described above) is in another domain that does not have a trust relationship with the domain where the account is being created. Local accounts cannot be used to logon to systems within the domain interactively, but can access the system's resources over the network. When you are finished, click **OK** to return to the **NEW USER** dialog box.
9. Click on the **DIALIN** Button. The **DIALIN INFORMATION** dialog box appears. Note: This option is only applicable when the Windows NT system is setup to handle remote connections.
   a) Click the **GRANT DIALIN PERMISSION TO USER** box if the user will be allowed to dialin to the system
   b) Select the appropriate call back option.
      i) **NO CALL BACK**. No call back is required to establish a dialin connection
      ii) **SET BY CALLER**. The system will prompt the user for a number.
      iii) **PRESET TO**. Enter a preset number for the server to use to perform the call back.
   c) When you are finished, click **OK** to return to the **NEW USER** dialog box.
10. Click the **ADD** button to add the new user and return to the User Manager dialog box.

Note: Depending on the version of Windows NT you are running, whether or not you are establishing local accounts on a Windows NT Workstation using User Manager or domain accounts on a Windows NT Server using User Manager For Domains, the properties/options available will vary.

E. How To Change Existing User Accounts

To make changes to an existing user account:

1. Open User Manager, select the appropriate user and from the **USER** menu choose **PROPERTIES** or hit enter or double click on the appropriate user. The **USER PROPERTIES** dialog box appears.
2. The **USER PROPERTIES** dialog box is essentially the same as the **NEW USER** dialog box. From this box changes can be made to the user account following the same steps as those for adding a new user.

10. USER RIGHTS POLICY

A. Overview

A User Right is a privilege for a user to perform a certain action on a Windows NT system such as managing the system's auditing policy or accessing all files on the system. A right applies to the entire system and a right overrides access permission set on an object. Rights should only be assigned to a user or group of users who require the additional access to system resources to perform their job, but who do not need all of the access required by a system administrator.

System administrators must be selective in granting rights to users. Where practical, access permissions should be assigned instead of granting rights. This is because permissions apply to specific objects and how they may be accessed, which provides tighter control, and rights apply across the entire system. For example, a system administrator would not give a user the Back up files and directories right, which allows all files to be seen and read, just because the user needs to read the files in one directory on the system. See the section on Group Management for tips on effectively administering rights using groups.

B. Types Of User Rights

The basic User Rights, or those that are most often assigned to users or groups of users are:

- Access this computer from network
- Backup files and directories
- Change the system time
- Force shutdown from a remote system
- Log on locally
- Manage auditing and security log
- Restore files and directories
- Shut down the system
- Take ownership of files or other objects
- Load and unload device drivers
- Add workstations to domain

In addition to the basic User Rights listed above, Windows NT offers advanced User Rights. These rights are normally reserved for programmers who would need the additional access to system resources and would not normally be granted to users and groups.

C. How To Set Or Adjust The User Rights Policy

To set or adjust the User Rights Policy:

1. Open User Manager and from the **POLICIES** menu choose **USER RIGHTS**. The **USER RIGHTS POLICY** dialog box appears.
2. From the **RIGHT** drop down box, select the right you wish to administer. Note: In order to view the **ADVANCED USER RIGHTS**, you will need to select the **SHOW ADVANCED USER RIGHTS** box.
3. If you wish to remove a user or group who has been granted the selected right, select the user or group and click the **REMOVE** button.
4. If you wish to grant the selected Right to a user or group, click the **ADD** button. The **ADD USERS AND GROUPS** dialog box appears. From the **LIST NAMES FROM** drop down box select the local system or domain whose user accounts database contains the users or groups you wish to add. Select the users (click the **SHOW USERS** button to display users) and groups you wish to add (if you select a group, you can click the **MEMBERS** button to see a list of users and global groups that are members of the selected group). Click the **ADD** button. Once you have granted the right to all the appropriate users and groups, click **OK** to return to the **USER RIGHTS POLICY** dialog box.
5. Once you have finished administering rights, click **OK** to return to the User Manager.

11. GROUP MANAGEMENT

A. Overview

As previously mentioned, a group is essentially an account containing other accounts in Windows NT. A user in a group is a member of the group and access permissions, rights, and restrictions assigned/granted to the group are assigned/granted to each of the Group members. Groups are an administrative tool used to provide a collection of users, with common needs, the permissions and rights they need to perform their job. For example, if a directory is established for the Payroll Department to hold their common files, it is much easier for a system administrator to have everyone in the Payroll Department in a group and then assign that group permissions on the directory and the files in it. Otherwise, the system administrator would have to go through and assign permissions to every user in the Payroll Department. In addition, groups can be used to restrict the access a collection of users have to certain objects. For example, the system administrator could utilize the Payroll group to prevent the users in the Payroll Department from printing to a printer in a remote location (because their data could potentially be very sensitive), while allowing access for all other users, by placing a deny ACE in the ACL for the printer.

It is normally easier to administer rights by granting them to groups and then making the users who need the right a member of the group. For example, if there are users who need to logon to a server locally, create a group called Local Logon, add the users to the group, and grant the Log on locally right to the group. This group could then be reused again should this group of users need some other right or access permission.

There are basically three types of groups in Windows NT, Local Groups, Global Groups, and Special Groups.

B. Local Groups

Local groups are maintained on a local system or domain and may have user accounts or global groups as members. At the local system level, local groups would be used to administer permissions and rights for the system on which they reside. At the domain level, local groups would be used to administer permissions and rights on Windows NT Servers within the domain where the groups reside. To summarize, local groups are only utilized in the user account database for the local system or domain where they are created.

Windows NT provides some built-in local groups each with established permissions and rights. At the local system level they are:

- Administrators - can fully administer the system.
- Power Users - can share directories and printers.
- Users - normal users.
- Guests - granted guest access.
- Backup Operators - can bypass file security in order to complete backups.

At the domain level, the built-in groups are:

- All listed above except Power Users.
- Server Operators - can manage domain servers.
- Account Operators - can manage user accounts and groups.
- Print Operators - can manage printers.
- Replicator - support file replication.

C. Global Groups

Global groups are maintained on a Windows NT domain, may have domain user accounts as members, and are used to administer domain users. System administrators can effectively use global groups to sort users based on their needs and then place their global group in the appropriate local groups to assign the group members the permissions and grant them the rights they need to perform their jobs. As mentioned, global groups can only have domain user accounts as members; no other groups can be members of a global group. This is because, the system administrator would assign permissions and grant rights to the local groups (because the local system or domain server holds the resources) and then make the global groups members of the local groups.

Windows NT provides two built-in global groups each with established permissions and rights. They are:

- Domain Admins - contains the domain administrator account by default and is a member of the domain level Administrators local group and the system level Administrators local group for Workstations in the domain.
- Domain Users - contains all the domain users.

D. Special Groups

Special groups are created by Windows NT for unique or specific purposes and can not be viewed, changed, or have members added to them in the User Manager. A users membership to a special group is determined by how they access resources on the system. Special groups may be assigned access permissions in some cases and may be seen when a system administrator is assigning permissions on Windows NT objects.

The following is a list of the special groups and a description of their membership:

- Network - any user connected to a system via the network.
- Interactive - any user logged on interactively at a local system
- Everyone - any user logged on to the system (both the Network and Interactive groups).
- Creator Owner - the user that created or took ownership of an object. Note: if the user was the system administrator or other user that is a member of the Administrators group, the Administrator group would be a member of the Creator Owner group.
- System - the Windows NT operating system.

The special group that system administrators must pay close attention to is the Everyone group. As stated above, all users logged on are a member of this group. Therefore, any access permissions assigned to the Everyone group, to allow or deny access to objects, are by default assigned to all users. For example, if there was a file that only a certain group of users should be able access, the system administrator could assign permissions to that group that allows access to the file and then assign permissions to the Everyone group that denies access to the file. Since Windows NT acts on all deny ACEs before grant ACEs, it would stop when it found the deny ACE and no one would be allowed access including the group with permissions assigned to grant access to the file.

E. How To Create Local Groups

To create a local group:

1. Open User Manager and from the **USER** menu choose **NEW LOCAL GROUP**. The **NEW LOCAL GROUP** dialog box appears.
2. Give the new group a name and description.
3. To add users or global groups (if the system is in a domain) click the **ADD** button and the **ADD USERS AND GROUPS** dialog box appears. From the **LIST NAMES FROM** drop down box select the local system or domain whose user accounts database contains the users or groups you wish to add access for. Select the users and groups you wish to add (if you select a group, you can click the **MEMBERS** button to see a list of users and global groups that are members of

the selected group). Once you have added all the appropriate users and groups, click **OK** to return to the **NEW LOCAL GROUP** dialog box.

4. If you wish to remove a user or group, select the user or group and click the **REMOVE** button.
5. Once you have finished, click **OK** to return to the User Manager.

F. How To Create Global Groups

To create a Global group:

1. Open the User Manager for Domains and from the **USER** menu choose **NEW GLOBAL GROUP**. The **NEW GLOBAL GROUP** dialog box appears.
2. Give the new group a name and description.
3. On the right side of the dialog box is a **NOT MEMBER** box with a list of domain users. Select the appropriate users and click the **ADD** button to move them to the **MEMBERS** box. You can move members to the **NOT MEMBERS** box by selecting the users and clicking the **REMOVE** button.
4. Once you have finished, click **OK** to return to the User Manager For Domains.

After groups have been created, they can be managed from the User Manager or User Manager For Domains. From the appropriate User Manager, select the group and from the **USER** menu choose **PROPERTIES**, hit enter or simply double click on the group. The **LOCAL/GLOBAL GROUP PROPERTIES** dialog box appears. This dialog box is essentially the same as the **NEW GROUP** dialog box and allows any change that can be made from the **NEW GROUP** dialog box except the group's name.

12. ACCOUNT POLICY

A. Overview

The Account Policy controls the password characteristics for all user accounts on a Windows NT system or a Windows NT domain. The characteristics set by the system administrator are global and all users are forced to adhere to them.

B. How To Set The Account Policy

To set or adjust the Account Policy:

1. Open User Manager and from the **POLICIES** menu choose **ACCOUNT**. The **ACCOUNT POLICY** dialog box appears.
2. Set the **MAXIMUM PASSWORD AGE**. You may select that the **PASSWORD NEVER EXPIRES** or you may select that the **PASSWORD EXPIRES** in 1 to 999 days.
3. Set the **MINIMUM PASSWORD AGE**. You may select that the **PASSWORD CAN BE CHANGED AGAIN IMMEDIATELY** or you may select that the **PASSWORD CAN BE CHANGED** again in 1 to 999 days.
4. Set the **MINIMUM PASSWORD LENGTH**. You may select to **PERMIT BLANK PASSWORDS** or you may select that the **PASSWORDS BE AT LEAST** 1 to 14 characters long.
5. Set the **PASSWORD UNIQUENESS** feature. You may select that a **PASSWORD HISTORY** is not kept or you may select that from 1 to 24 **PASSWORDS ARE REMEMBERED**. Note: For this feature to be effective, you must specify an age value for the **MINIMUM PASSWORD AGE**.
6. Set the **ACCOUNT LOCKOUT** feature. You may select that **NO ACCOUNT LOCKOUT** occurs or you may select that **ACCOUNT LOCKOUT OCCURS AFTER** 1 to 999 **FAILED LOGON ATTEMPTS**. You must also enter a value for the **COUNT RESET**. The **COUNT RESET** value represents the number of minutes that must pass between any two failed logon attempts to ensure that lockout will not be in affect. The number of minutes may be from 1 to 99,999.
7. Set the **LOCKOUT DURATION** feature. You may select that the duration be **FOREVER**, that is until the system administrator unlocks the user account in the User Manager, or you may select that the duration be from 1 to 99,999 minutes.
8. Select whether or not **USERS MUST LOGON IN ORDER TO CHANGE THEIR PASSWORD**. Selecting this feature prevents users from logging on with an expired password. However, it also prevents users from logging on if their **USER PROPERTIES** are set to force them to change their password at next logon.
9. When you have finished making your selections, click **OK** to return to User Manager.

C. Some things to remember about the Account Policy.

1. Changes to the Policy do not affect users until their next logon.
2. Changes to the Minimum Password Length do not affect users until they change their password again. Therefore, if the Policy was set to allow blank passwords and was changed to require at least six characters for example, users will not be forced to use a six character password until they change their password again. This can be corrected by changing the properties for all user accounts to force a password change at next logon.
3. In the Account Policy for User Manager For Domains, there is an additional feature that can be selected to Forcibly Disconnect Remote Users When their Logon Hours Expire. If this option is selected, the system will warn the user prior to the hours expiring and then disconnect them when the hours do expire. If the feature is not selected, users are only warned.

13. USER PROFILES

A. Overview

A User Profile is a configuration file that contains settings for a user's desktop environment. Specifically, the User Profile contains settings for the following areas:

- Program Manager
- File Manager
- Command Prompt
- Print Manager
- Control Panel Options
- Accessories
- Third-Party Windows-NT Applications
- Online Help Bookmarks

The settings saved in the profile, for each of the areas listed above, would include:

- User-definable settings.
- All settings saved by the Save Settings on Exit and Save Settings Now commands.
- Network connections established in File Manager, Explorer, and Print Manager.
- Bookmarks placed in the Windows NT Help System.

The use of User Profiles can be advantageous for both system administrators and users. For system administrators, it is a way to manage a user's environment. For users, it is a way to ensure they have a common desktop environment no matter where they logon (using server-based profiles) or ensure they have their own personal environment on a particular system (using profiles stored locally).

B. Types Of User Profiles

There are four types of Use Profiles:

1. **Mandatory** - a system administrator can create a profile and then force a user or multiple users to utilize it when they logon. While logged on, users can change settings, but the changes made cannot be saved in the Mandatory Profile and are lost when the user logs off. As described latter, Mandatory Profiles can be used by system administrators to restrict a user's abilities.
2. **Personal** - With a Personal Profile, users can change settings and have them saved in the profile when they log off.
3. **User Default** - This is the default profile used by Windows NT for a user if they have not been assigned a profile and it is their first time to logon, if the user's assigned profile cannot be accessed, or if the user is logging on as a Guest. The user can make changes to settings and if they are not logged on as Guest, the changes are saved. The next time the user logs on, the modified default profile becomes their Personal Profile.
4. **System Default** - This profile is utilized by Windows NT when no one is logged into the system interactively and presents the user the logon dialog box.

User profiles can be stored locally or remotely on a server. Profiles stored locally can only be accessed and used on the system where they are stored. Profiles stored remotely on a server can be accessed and used no matter where the user logs on. Server-based profiles can be either personal profiles or mandatory profiles and are in most cases the best to use. A server-based profile will give a user the same desktop environment no matter which system is being logged on from. With a mandatory server-based profile, a system administrator can ensure that the restrictions established are always implemented. In addition, the same mandatory profile can be used for multiple users across the network. However, the system administrator must ensure that the mandatory profile is always accessible. If a user is assigned a mandatory profile and Windows NT cannot access it during the logon process, the user will not be able to logon. If the user is assigned a personal profile and Windows NT cannot access it during the logon process, then the default profile is used.

C. How To Create And Modify User Profiles

User profiles are initially created and changed with the User Profile Editor. The User Profile Editor can only be run by a member of the Administrator Group. The following four sections need to be completed in the Profile Editor:

1. **PERMITTED TO USE PROFILE** - assign the appropriate users or groups.
2. **PROGRAM MANAGER SETTINGS** - Controls the following:
   a) Which applications are started during logon.
   b) Whether or not the user can access Common Program Groups.
   c) Whether or not the user can save changes, made during the logon session, to the profile.
   d) Whether or not the user can use the Run command in the File menu.
3. **PROGRAM GROUP SETTINGS** - Restricts the user's ability to make changes to personal program groups. System administrators can lock groups so that no changes are made or they can unlock groups and allow one of the following four access permissions:
   a) Make Any Change
   b) Create / Delete / Change Program Items
   c) Change All Program Item Properties
   d) Change Program Item Properties Except Command Line

One final note on profiles, profiles have no effect when the user logs on from a DOS/Windows workstation.

14. LOGON SCRIPTS

A. Overview

Logon scripts are batch files or executable programs that are assigned to users and executed by Windows NT whenever the user logs on. Logon scripts are not as powerful as user profiles, but can be used to make network connections, start applications, and configure some of a user's environment. In addition, unlike user profiles logon scripts can be used when a user logs on from a DOS/Windows workstation.

B. Locations

The default logon script directory is:
WINNT\SYSTEM32\REPL\IMPORT\SCRIPTS.

Logon scripts can also be placed in a directory on a Windows NT Server that may be replicated to other servers. The default replication directory for logon scripts is:
WINNT\SYSTEM32\REPL\EXPORT\SCRIPTS

If the system administrator places all logon scripts in the directory for replication, the Replicator Service can be used to synchronize script files among multiple servers. This is advantageous because in a domain environment the system administrator can keep all logon scripts in a central location and users can have their logon validated by anyone of the servers acting as a Domain Controller.

15. AUDITING TOOLS

A. Overview

System administrators with large Windows NT systems will probably want and need to purchase a good third party security analysis tool. These tools can assist in checking the overall security of a Windows NT system. A good security analysis tool can point out weaknesses in the security posture of the system, provide detailed reports, use a knowledge base to provide tips, perform ongoing system monitoring, and allow the system administrator to focus on certain security areas or objects. Tools are available that will allow system administrators to analyze:

- Registry Permissions
- Trust Relationships
- Audit Policies
- User Rights
- Domain Security
- File and Directory Permissions
- Share Permissions
- Event Logs
- Printer Permissions
- Password Management, including the ability to check for easy to guess passwords
- Logfailures
- C2 Security (Microsoft provides a C2 Config utility with the Windows NT Resource Kit)

B. Some Suggestions

New products are constantly being released for Windows NT security analysis. Some vendors to check are:

- Intrusion Detection, Inc., www.intrusion.com
- Axent Technologies, www.axent.com
- Somarsoft, Inc., somarsoft.com
- Raxco, Inc., www.raxco.com

16.WHERE TO FIND ADDITIONAL INFORMATION

A. Web Sites

1. CMP's NT Solution Center - http://techweb.cmp.com/ecg/nt

2. Win NT Update - http://www.zdnet.com/wsources/update/ntupdfr.html

3. Windows NT Resources - http://www.winntmag.com/resources

4. Windows NT Resources Site - http://www.chancellor.com/ntmain.html

5. Microsoft Windows NT Page for Help Files, Service Packs, etc.
   http://www.microsoft.com/NTWksSupport/default-sl.htm

6. Frank's Windows Page - http://www.conitech.com/windows/index.html

7. Microsoft's Hardware Compatibility List for Windows NT 4.0 -
   http://www.microsoft.com/isapi/hwtest/hsearchn4.idc

8. Lifeform WindowsNT Resource
   http://www.lifeform.demon.co.uk/ntres.html#security

9. How to Create Internet Site with Windows NT only -
   http://www.neystadt.org/winnt/site.htm

10. Beverly Hills Software's Windows NT Resource Center - http://www.bhs.com

11. Digital's Windows NT Home Page -
    http://www.windows.digital.com/INDEX.HTP

12. Windows NT Web Server Tools -
    http://www.primenet.com/~buyensj/ntwebsrv.html

13. Rick's Windows NT Info Center - http://rick.wzl.rwth-aachen.de/rick

14. Microsoft's Windows NT Server Page -
    http://www.microsoft.com/ntserver/default.asp

15. Microsoft's Windows NT Workstation Page -
    http://www.microsoft.com/ntworkstation/default.asp

16. File Mine - http://www.filemine.com

17. WindowsHelper - http://www.techweb.com/helper/thfeature/winhelp.html

18. Somarsoft, Inc. - http://www.somarsoft.com

19. Miscellaneous Security Documents - http://www.alw.nih.gov/Security/security-docs.html

20. Computer Security Resource Clearing House - http://csrc.nist.gov

21. Security Info Page - http://www.securityinfo.com

B. Books

1. Windows NT 3.5 Guidelines for Security, Audit, and Control by Microsoft Press - ISBN 1-55615-814-9, (A little dated, but still an excellent book.)

2. Windows NT Security Guide by Stephen A. Sutton - ISBN: 0-201-41969-6

3. Network & Internet Security by Vijay Ahuja - ISBN: 0-12-045595-1

4. Microsoft Windows NT Workstation Resource Kit Version 4.0 - ISBN: 1-57231-343-9

5. Microsoft Windows NT Server Resource Kit Version 4.0 - ISBN: 1-57231-344-7

6. Microsoft Windows NT Server Resource Kit Version 4.0, Supplement 1 - ISBN: 1-57231-559-8

7. Microsoft Windows NT Resource Kit For Windows NT Workstation and Windows NT Server Version 3.51 - ISBN: 1-55615-926-9

8. Running Microsoft Windows NT Server 4.0 by Charlie Russell and Sharon Crawford - ISBN: 1-57231-333-1

9. Inside Windows NT by Helen Custer - ISBN: 1-55615-481-X

10. Inside the Windows NT® File System by Helen Custer - ISBN: 1-55615-660-X

11. Microsoft Windows NT 4.0 Upgrade Training - ISBN: 1-57231-528-8

12. Microsoft Internet Information Server Training - ISBN: 1-57231-425-7

13. Windows NT 4.0 Server Unleashed by Jason Garms - ISBN 0-672-30933-5

14. Inside Windows NT Workstation by George Eckel - ISBN 1-56205-583-6

Appendix A - Permission Tables

Table 1 - Basic Permissions that may be assigned to files

	No Access	Read	Change	Full Control
View File's Data		YES	YES	YES
View File's Attributes		YES	YES	YES
Execute File (if it is a program)		YES	YES	YES
View File's Owner & Permissions		YES	YES	YES
Change File's Attributes			YES	YES
Change Data In The File And Add Data To The File			YES	YES
Delete File			YES	YES
Take Ownership Of File And Change File Permissions				YES

Table 2 - Custom Permissions that may be assigned to files when the basic permission "Special Access" is selected

	READ	WRITE	EXECUTE	DELETE	CHANGE PERMISSION	TAKE OWNERSHIP	FULL CONTROL
View File's Owner & Permissions	YES	YES	YES				YES
View File's Data	YES						YES
View File's Attributes	YES		YES				YES
Change File's Attributes		YES					YES
Change Data In The File And Add Data To The File		YES					YES
Execute File (if it is a program)			YES				YES
Delete File				YES			YES
Change File Permissions					YES		YES
Take Ownership Of File						YES	YES

Table 3 - Basic Permissions that may be assigned to directories

	NO ACCESS	LIST	READ	ADD	ADD + READ	CHANGE	FULL CONTROL
View File Names In A Directory		YES	YES		YES	YES	YES
View Directory Attributes		YES	YES	YES	YES	YES	YES
Change To Subdirectories		YES	YES	YES	YES	YES	YES
Change Directories Attributes				YES	YES	YES	YES
Add Subdirectories And Files				YES	YES	YES	YES
View Directory's Owner And Permissions		YES	YES	YES	YES	YES	YES
Delete Directory						YES	YES
Delete Files Or Empty Subdirectories in Directory							YES
Change Directory Permissions							YES
Take Ownership Of Directory							YES

Table 4 - Custom Permissions that may be assigned to directories when the basic permission "Special Directory Access" is selected

	READ	WRITE	EXECUTE	DELETE	CHANGE PERMISSION	TAKE OWNERSHIP	FULL CONTROL
View File Names In A Directory	YES						YES
View Directory Attributes	YES		YES				YES
Add Subdirectories And Files		YES					YES
Change Directories Attributes		YES					YES
Change To Subdirectories			YES				YES
View Directory's Owner And Permissions	YES	YES	YES				YES
Delete Directory				YES			YES
Change Directory Permissions					YES		YES
Take Ownership Of Directory						YES	YES

Table 5 - Permissions for directories and their effects on files

	NO ACCESS	**LIST**	**READ**	**ADD**	**ADD + READ**	**CHANGE**	**FULL CONTROL**
View File's Owner & Permissions			YES		YES	YES	YES
View File's Data			YES		YES	YES	YES
View File's Attributes			YES		YES	YES	YES
Change File's Attributes						YES	YES
Change Data In The File And Add Data To The File						YES	YES
Execute File (if it is a program)			YES		YES	YES	YES
Delete File						YES	YES
Change File Permissions							YES
Take Ownership Of File							YES

Table 6 - Permissions that may be assigned to shared directories

	NO ACCESS	READ	CHANGE	FULL CONTROL
View Subdirectory and File Names		YES	YES	YES
View File's Data And Attributes		YES	YES	YES
Execute File (if it is a program)		YES	YES	YES
Change To Subdirectories		YES	YES	YES
Add Subdirectories And Files			YES	YES
Change Data In The File And Add Data To The File			YES	YES
Change File's Attributes			YES	YES
Delete Files Or Empty Subdirectories in Directory			YES	YES
Change Directory, Subdirectory, Or File Permissions (NTFS)				YES
Take Ownership of Directory, Subdirectories, Or Files (NTFS)				YES

Table 7 - Permission Abbreviations

PERMISSION	ABBREVIATION
Read	R
Delete	D
Write	W
Change Permission	P
Execute	X
Take Ownership	O

Table 8 - Permissions that may be assigned to Registry keys and subkeys

PERMISSION	DESCRIPTION
Read	Read the key.
Full Control	Read, edit, and take ownership of the key.
Special Access	See individual permissions below
Query Value	Read a value entries from a key
Set Value	Set value entries in a key
Create Subkey	Create subkeys on a key
Enumerate Subkeys	Identify the subkeys of a key
Notify	Audit notification events from a key
Create Link	Create a symbolic link in a key
Delete	Delete a key
Write DAC	Write to the ACL (assign a permission) of a key
Write Owner	Take ownership of a key
Read Control	Access the security assigned to a key

Table 9 - Permissions that may be assigned to printers

	No Access	**Print**	**Manage Documents**	**Full Control**
Print Documents		YES		YES
Control Document Settings			YES	YES
Pause, Resume, Restart, or Delete Print Jobs			YES	YES
Change The Order Of Print Jobs				YES
Pause Or Resume Printer				YES
Purge Printer				YES
Change Printer Properties				YES
Delete A Printer				YES
Change Printer Permissions				YES